資歷架構 Qualifications Framework

Vocational Qualifications Pathway (VQP) for Internet of Things (IoT)

Area / Job Level	Internet of Things (IoT)
Master Level	*The ICT practitioners at this level are mainly responsible for decision-making processes. They oversee the entire IT operations and strategic development direction in the organizations. The Professionals at this level are required to possess broad corporate perspective, good communication skills and in-depth technology knowledge.*
Relevant Job Titles	Director of IoT
	Chief Digital Officer (IoT)
Specialist Level	*The ICT practitioners at this level are mainly involved in managerial processes. They may work with individual technical departments and manage those departments by applying their technical and managerial skills. The major tasks performed by the professionals at this level are to manage individual activities and project segments, and to lead the projects towards completion within the assigned budget and stipulated deadline.*
Relevant Job Titles	IoT Software Engineer
	IoT Solution Architect
	IoT Business Manager
Practitioner Level	*The ICT practitioners at this level manage certain parts of technical processes depending on their subject matter expertise. The professionals at this level may be sub-degree graduates or those who possess certain work experience in the field.*
Relevant Job Titles	IoT Support Engineer
	Assistant IoT Developer
Support Level	*The ICT practitioners at this level provide entry-level technical operation and support functions depending on their subject matter expertise. The practitioners at this level may be S6 graduates with relevant ICT skills and knowledge or those who possess little work experience in the field.*
Relevant Job Titles	Computer Operator
	User Support Staff
	Technical Support Staff (TSS)
	Field Technician
	Help Desk Operator

Proposed Competency Requirements (Internet of Things - Master Level)

Relevant Job Titles:

- Director of IoT / Chief Digital Officer (IoT)

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
IoT policies and strategies	1. Develop and manage the IoT strategy, operational and engagement plans	▪ Define a system migration plan ▪ Develop procedures to implement incident response plan ▪ Formulate IT strategies and policies ▪ Review the emerging technologies and cross-functional strategies	111155L6 111170L5 ITSWSM603A 111207L6	Obtain qualification via training programmes (QF Level 6)
	2. Define the business model for how business operations can be enabled in IoT	▪ Formulate business strategies and policies ▪ Identify and evaluate information technologies that support the objectives of an organisation	111201L6 111202L6	
	3. Coach and enable team to identify and proactively engage with key customer, technical decision makers and influencers to help unblock technical obstacles	▪ Determine technology mix for the design and development of embedded software systems ▪ Conduct solicitation planning	111126L6 111197L5	

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Quality Assurance and information security for IoT	4. Ensures consistency and quality through capturing, sharing, and adherence of standards and best practices.	▪ Review and comply with organisational policies and procedures, relevant laws and regulatory requirements ▪ Define data governance policies and architecture principles ▪ Review the ethical and social issues for IT applications ▪ Set policy to control data security and privacy	111205L6 111123L6 111208L6 111206L6	(Continued) Obtain qualification via training programmes (QF Level 6)
Strategic management	5. Overview and review work on the team (Generic Skills)	▪ Lead and motivate a team ▪ Delegate responsibilities ▪ Manage changes	ITSWGS604A ITSWGS606A ITSWGS613A	

Proposed Competency Requirements (Internet of Things - Specialist Level)

Relevant Job Titles:

- IoT Software Engineer / IoT Solutions Architecture / IoT Business Manager

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Management and development of IoT System	1. Manage the strategy and development of Internet of Things (IoT) ecosystem of the organization, including platform requirements, customer experience and market strategies.	▪ Master the Internet of Things development technology ▪ Design and develop data management tools and services to manage the target data based on different requirements	107218L5 111142L6	Obtain qualification via training programmes (QF Level 5)
	2. Ensure data and information about the organization's IoT portfolio is clearly understood both internally and externally in the most professional, accessible and secure ways	▪ Define metrics to ensure that a technology architecture meets the business goals ▪ Develop and perform data acquisition and collection processes and conduct pre-processing and exploratory data analysis	111127L5 111131L5	
	3. Carry out designing, coding and testing features of IoT devices	▪ Evaluate the results of application security assessment for improvement recommendation ▪ Perform inspection for the programme code and software documents ▪ Develop test plans for various levels of testing	111173L5 ITSWDM506A ITSWDM507A	

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Project Management (IoT)	4. Monitor and control IoT project execution according to the defined plan and objectives	▪ Monitor and control project execution ▪ Monitor, control and update project schedule ▪ Manage the execution of a project quality management plan	ITSWPM605A ITSWPM504A ITSWPM509A	(Continued) Obtain qualification via training programmes (QF Level 5)
	5. Research and recommend technologies to improve current systems and apply subject matter expertise and thought leadership for shaping the organization's long-term IoT strategy	▪ Analyze the available solutions from IT service providers ▪ Conduct source selection and/or contract development	111199L4 ITSWPM523A	

Proposed Competency Requirements (Internet of Things - Practitioner Level)

Relevant Job Titles:

- IoT Support Engineer / Assistant IoT Developer

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Installation and configuration of hardwares and softwares for IoT devices	1. Assist in the design and development of IoT software with clear understanding of sensors and network communication among digital devices	▪ Install and configuration of internet server application ▪ Understand key characteristics of embedded software systems ▪ Plan and develop the analytics and modeling tools ▪ Manage and maintain the programme source	111120L4 ITSWAR521A 111147L6 ITSWDM505A	Obtain qualification via training programmes (QF Level 4)
	2. Coordinate with end-users, sites contacts, vendors and in-house cross functional teams for implementing IoT projects	▪ Perform system testing against user, technical and hosting requirements ▪ Perform installation, configuration and testing of network equipment and devices ▪ Define user requirements	111160L4 111106L3 111162L4	
	3. Perform trouble-shooting with IoT devices	▪ Analyse the performance, latency and accessibility of systems ▪ Perform network testing ▪ Apply diagnostic and troubleshooting skills to solve hardware, software and networking related issues	111130L4 111107L4 111121L4	

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Quality assurance and information security (IoT)	4. Implement system operational security and ensure data privacy.	▪ Apply encryption technology to send data ▪ Prepare system operation documentation ▪ Implementing monitoring equipment to monitor infrastructure failure and security breaches	107233L4 111200L4 111429L4	(Continued) Obtain qualification via training programmes (QF Level 4)

Proposed Competency Requirements (Internet of Things - Support Level)

Relevant Job Titles:

- Computer Operator / User Support Staff / Technical Support Staff (TSS) / Help Desk Operator / Field Technician

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Network Support	1. Network Support	▪ Install and configure client/server application ▪ Configure WAN connection ▪ Troubleshoot network issues	107882L3 107883L3 107884L3	Obtain qualification via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS010L3)
Network and Security Support	2. Network and Security Support	▪ Build a small wireless LAN ▪ Install and configure network components/devices ▪ Install and configure client/server application ▪ Strengthen workstation protection ▪ Troubleshoot web browser and connection issues	107879L2 107880L2 107882L3 107891L3 107909L3	Obtain qualification via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS016L3)
System Security Support	3. System Security Support	▪ Create and maintain user accounts on server ▪ Configure user access control on server ▪ Administer system security	107885L2 107886L3 107888L3	Obtain qualification via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS009L3)
User Support	4. User Support	▪ Provide support to mobile device users ▪ Troubleshoot client device hardware issues ▪ Perform remote support	107904L3 107905L3 107907L3	Obtain qualification via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS012L3)

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Web Support	5. Web Support	▪ Troubleshoot web browser and connection issues ▪ Maintain website performance ▪ Build simple website using content management systems ▪ Maintain website	107909L3 107910L3 107911L3 107912L3	Obtain qualification via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS013L3)
Application Support (Technical Support)	6. Application Support	▪ Coordinate application change requests with developer ▪ Install and configure Apps on client devices ▪ Perform application configuration ▪ Troubleshoot application problems	107872L2 107873L2 107874L2 107875L3	Obtain qualification via training programmes (QF Level 2) Or RPL Mechanism (QF Level 2 RPL Cluster: ITOS003L2)

Specification of Competency Standards
for the Retail Industry
Unit of Competency

Functional Area - Website Design and Development

Title	Master the Internet of Things development technology
Code	107218L5
Description	In the process of website design and development, through the unified format or standard of information obtained from the Internet of Things (IoT) to enable communicate and information transfer between various systems so as to achieve diversified information at the website.
Level	5
Credit	6 （For Reference Only）
Competency	Performance Requirements 1. Understand the concept of IoT • Understand the basic structure of the three layers of IoT including the perception layer (Device), network layer (Connect), application layer (Manage) • Master sensing technology and identification technology • Understand the network communication technology, the variety of different communication range and transmission rate of wireless communication network • Understanding heterogeneous network integration technology for IoT • Analyse case studies for future development and challenges 2. Master the development of IoT technology • Utilize devices with sensing, identification and communication capabilities to sense and monitor different scenarios • Apply the information collected by the perceptual layer to transmit to the Internet or wireless communication network • Implement integration of professional and technical networking between the IoT and the industry according to the different needs of the application software development. • Consolidate real-time information and status collected by heterogeneous network technologies, devices and packet formats 3. Exhibit professionalism • Comply with the requirements of the Personal Privacy Ordinance in data collection and process. • Ensure no disturbance of IoT with a large number of different equipment so as to achieve the best service quality and information security.
Assessment Criteria	The integrated outcome requirement of this UoC is the ability to: • Understand the three layers of the basic architecture of IoT • Consolidate real-time information and status collected by heterogeneous network technologies, devices and packet formats • Master the development technology of IoT. Implement perception monitoring, transmission of information to the Internet, technology integration of IoT and the industry and the development of the corresponding application software.
Remark	

Specification of Competency Standards
for the Retail Industry
Unit of Competency

Functional Area - Transaction Security Technology

Title	Apply encryption technology to send data
Code	107233L4
Description	Apply technical means to change the important information into garbled (encrypted) transmission. Upon reaching the destination, apply the same or different means to restore (decryption).
Level	4
Credit	12 （For Reference Only）
Competency	Performance Requirements 1. Master the basic concepts of encryption technology • Explain the basic terminology of encryption techniques, including: o Plaintext o Ciphertext o Encryption o Decryption o Encryption Algorithm o Decryption Algorithm o Sender o Receiver o Key o Eavesdropper o Cryptanalysis o Cryptanalyst o Passive Attack o Active Attack 2. Apply encryption technology • Apply symmetric encryption technology o Understand the five basic components of symmetric encryption technology ▪ Plaintext ▪ Encryption algorithm ▪ The key ▪ Ciphertext ▪ Decryption algorithm o Understand and select appropriate data encryption algorithms ▪ Data encryption standard (DES) - the most widely used algorithm ▪ Triple DES ▪ Advanced Encryption Standard (AES) ▪ Bluefish algorithm ▪ RC5 algorithm • Apply asymmetric encryption technology o Understand the composition of the public key cryptography system, including: ▪ Plaintext ▪ Encryption algorithm ▪ Public key and private key ▪ Ciphertext ▪ Decryption algorithm o Apply the public key cryptography

Functional Area - Transaction Security Technology

	▪ Encryption / decryption: The sender encrypts the message with the recipient's public key o Digital Signature: The sender signs the message with its private key. The signature can be generated by encrypting the entire message or by encrypting a small piece of information for the message, where the small data block is the function of the entire message ▪ Key exchange: communication exchange key for both parties ▪ RSA algorithm o Recognize other public key encryption algorithms, including: ▪ ELGamal algorithm ▪ Backpack encryption algorithm o Master the key management technology ▪ Key Distribution Technology ▪ Key authentication technology ▪ The Certification Authority (CA) verifies that a public key belongs to a particular entity (A person or a network entity) ▪ Digital certificate • Recognize Secure Sockets Layer (SSL) encryption technology o SSL is a widely implemented public key encryption technology, the main types include: ▪ No client SSL ▪ Configure the clientless SSL for the VPN device ▪ Network to network ▪ Host to network 3. Exhibit professionalism • Introduce the most suitable for the corporate encryption technology. • Abide by professional conduct and prevent any fraud in the use of encryption technology. • Comply with the relevant legal requirements in the use of encryption technology.
Assessment Criteria	The integrated outcome requirement of this UoC is the ability to: • Understand the basic concepts of encryption technology • Master the basic encryption algorithm design principles • Complete the basic encryption calculation and process data transmission.
Remark	

Unit of Competency

Functional Area: Application Support

Title	Coordinate application change requests with developer
Code	107872L2
Range	This unit of competency applies to IT support personnel. Many systems are tailor-built due to special features and functions needed and canned packages cannot provide. The development work may be internal or external. As errors are being identified and new functions are required, a single contact point to coordinate with developers is required. This UoC will synonymously use “change request” for either error report and functional change request.
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge for coordinating application change requests with developer • Possess good interpersonal and communication skills for liaising with users and developers • Possess basic knowledge of change management concept • Possess good knowledge of the organisation’s change record system • Good teamwork attitude, self-disciplined and resourceful 2. Coordinate application change requests with developer • Received change request from user by “change request form” • Verify details of change request and perform initial filtering based on organisation’s change control procedure • Record the change request into internal record system with a change control ID number • Forward to supervisor to approve the change request or error report • Agree with change controller and allocate the level of priority for the change request • Forward change request to developer with indication of priority level • Liaise new change request with developer • Gather details of change request for developer • Acquire assigned reference details from developer and timeline for completion of work • Update developer given reference details to corresponding change request • Regularly monitor change request and its status. Contact developer for status may be required • Liaise with users relating to change requests, such as: • Provide status of change such as: accepted, rejected, ref. ID, etc. • Developer need for extra details related to the change request • Notify change request has been completed by developer • Acquire feedback to determine whether the change request completed to user’s expectation • Regularly monitor change request and its status • Update change request records with status of different stages of processing • Request change controller to close the change request on work completion when user is satisfied with delivered changes 3. Exhibit professionalism • Apply industry best practices for change management process and follow the organisation change control procedures to ensure all change control records are well maintained and updated • Take responsibility and accountable for coordination work and be impartial between users and developers regarding change requests

Unit of Competency

Functional Area: Application Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand change request made by users and can accurately record it into the organisation's change control record system • Convey adequate details of change request to developer that enable them to accurately assess the viability and plausibility of performing requested changes and can give an estimate of completion time • Monitor progress of change requests systematically in such a manner where important/critical change requests demand more frequent follow up and less critical ones are reported on scheduled dates
Remark	

Unit of Competency

Functional Area: Application Support

Title	Install and configure Apps on client devices
Code	107873L2
Range	This unit of competency applies to IT support personnel who are responsible for installing software applications (Apps) on different computing clients such as: personal computers (PC), notebooks, tablets and smartphones. When installing Apps for user some minimal training on use of the Apps would be needed
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for installing and configuring Apps on client device:
	• Possess good troubleshooting skills
	• Possess basic training skills
	• Possess basic knowledge of operating different computing clients
	• Possess good knowledge of installing software application
	• Possess basic knowledge of reading technical manual and following software installation and configuration instructions
	• Possess basic knowledge of the organisation health and safety guideline
	2. Install and configure Apps on client devices
	• Comprehend the software installation request from supervisor or user
	• Prepare for installation
	  • Comprehend a basic function overview, installation details and configuration details of the Apps
	  • Obtain installation media of the Apps
	  • Ensure the client devices conform to the minimum hardware requirements and sufficient storage space
	  • Locate or purchase the Apps' installation key or license, if required
	• Prepare the installation media
	  • For PCs and notebooks, mount installation media
	  • For tablets and smartphones, locate the Apps in the "market store" of the mobile platform. Example; IOS = App Store, Android = Play store, etc.
	• Follow the installation instructions of the Apps during the installation
	• Enter the license or installation key, if required
	• Configure the Apps with required settings that complied with the organisation security policy. Extra care should be paid to mobile Apps to avoid giving unnecessary authorisation to access device and personal information
	• Perform simple test to ensure the Apps can function normally in the expected manner. Troubleshoot any error messages during the installation and find rectification solutions before restarting installation
	• Complete internal documents and record configuration setting in accordance with the organisation's procedure
	3. Exhibit professionalism
	• Possess services attitude with desire to assist users with problems
	• Follow organisation safety guidelines and procedures when performing installation and configuring Apps on client devices

Unit of Competency

Functional Area: Application Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Perform preparation for installation process • Complete installation and configuration of Apps on the client device that meets the need of user and complied with the organisation security standards • Provide sufficient instructions or training to the user to enable them to operate the App with minimum problem
Remark	

Unit of Competency

Functional Area: Application Support

Title	Perform application configuration
Code	107874L2
Range	This unit of competency applies to IT support personnel who are responsible for supporting application configuration on different computing clients. The configurations are performed either at initial application installation or when there is a changed need requested by users or organisation wide. Configuration can be of different level ranging from simple cosmetic adjustment match individual users need to functional and features specific configuration which applied to companywide. For example, all pdf readers must support multi-language (English and Chinese) and has commenting functions.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for performing application configuration
	• Possess good reading skills to understand technical manual and follow software installation and configuration instructions
	• Possess basic training skills
	• Possess basic knowledge of operating different computing clients
	• Possess good knowledge of installing software, configuring applications and script programming
	• Possess basic knowledge of application testing
	2. Perform application configuration
	• Comprehend the application configuration requirement from work order or from user request
	• Review vendor documents to determine whether the required changes/configuration is available and can be performed on the application
	• Comprehend from appropriate technical documents, from vendor or other sources, to determine how configuration is performed on the application, such as:
	  • Menu driven within the application
	  • Direct editing of configuration file
	• For menu driven configuration method, locate which menu and what option settings
	• For configuration file settings method, identified name of configuration file and used appropriate editor to add/change settings on the file which configures the functions required by the user
	• After completed the configuration, perform appropriate tests to ensure the application functions are performing as required
	• Where necessary, provide operation instructions and/or provide basic tutorial to users on usage of configured functions
	• Complete internal documents and record configuration setting in accordance with the organisation’s procedure
	3. Exhibit professionalism
	• Committed to ensure completed work is free from error and function as required
	• Follow organisation safety guidelines and procedures when performing configuration work

Unit of Competency

Functional Area: Application Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Fully comprehend the configuration requirements and are well prepared for the configuration work, identified of where, and how to make the required configuration settings on the application • Perform the required configuration and satisfactorily test the application before release for general use • Complete the after configuration document in accordance with the organisation procedure and provide sufficient instructions or coaching to users on use of configured functions
Remark	

Unit of Competency

Functional Area: Application Support

Title	Troubleshoot application problems
Code	107875L3
Range	This unit of competency applies to IT support personnel who are responsible for application support. When users encounter application issues they request help from support team. The support personnel general responsibility includes troubleshoot and collect necessary information to be forwarded to application developer or vendor when reporting the problem. Additionally, the support personnel will provide advice and/or attempt to adjust configuration (system or application) to enable the application function or to bypass the problem and enable the user to continue with work.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for troubleshooting application problems • Possess good interpersonal skills that can communicate effective with different level of users • Possess good application troubleshooting skills • Possess basic knowledge of organisation’s application support guidelines and procedure • Possess basic knowledge of the internal problem recording system

Unit of Competency

Functional Area: Application Support

Competency	2. Troubleshoot application problems
	• Patiently listen to user or read problem report on symptoms of application problem and explain the actions will be performed and reason for the actions
	• From internal records, from user, or from the client system, gather as much as possible on details relating to the problem application, including but not limited to the following:
	  • Type of application
	  • Hardware, environment and compatibility requirement
	  • Configuration details
	  • Functions and features of the application
	  • Version/release number
	• Collect various messages related to the application problem, include:
	  • System log
	  • Application log
	  • Error messages from the application
	• Reconstruct the problem and analyse from available information to determine cause of problem, such as:
	  • Installation and configuration problem
	  • Startup problem
	  • Insufficient system resource
	  • Incorrect input or output
	  • User incorrect operation
	• During the recreation of the problem, record all actions performed, and/or capture all input and output, which will be forwarded to the application developer or vendor to assist application correction and for further detail analysis when required
	• Attempt to correct or bypass the problem by performing some of following actions:
	  • Reconfigure the application
	  • Uninstall and re-install the application
	  • Adjust system resource for the application
	• Perform simple tests to ensure the problem is corrected or bypassed before return it for user to use
	• Report the problem to application developer or vendor and forward the collected packaged details that include error messages, logs details, input and output details
	• Complete the internal record keeping procedure in accordance with the organisation guidelines and requirements
	3. Exhibit professionalism
	• Possess customer services attitude with desire to assist users with problems

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Communicate effectively with user to understand the issues of the application and collect sufficient information to re-create the problem • Identify the cause of the application problem and follow the organisation procedures and guidelines to collect sufficient details that can be used for further analysis and can be forwarded to application developer or vendor to assist with correction of the application • Provide suitable advice or perform appropriate setting corrections to application or system to enable it to continue function so that the user can continue with his/her work
Remark	

Unit of Competency

Functional Area: Network Support

Title	Build a small wireless LAN
Code	107879L2
Range	This unit of competency applies to junior IT personnel who are involved with construction of the organisation's network infrastructure. The main duties include installing, configuring of small wireless local area network (LAN) as well as performing user training on the use of the wireless LAN. However, during the planning and network design and sourcing of equipment for the wireless LAN he/she may be required to provide advice and assistance.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge to build a small wireless LAN:
	• Possess good communication and interpersonal skills
	• Possess good knowledge of basic training skills
	• Possess good knowledge of different network and wireless security risks
	• Possess good knowledge of wireless LAN components and their functions
	• Possess good knowledge of how to acquire technical manuals on wireless LAN equipment
	• Understand the network needs of users and the organisation
	• Possess good knowledge on use of network testing software
	2. Building a small wireless LAN
	• Comprehend and assess the wireless LAN design diagram. Confirm and raise any concerns or suggestions with the designer or supervisor before purchase of equipment or install work. Area where he/she may assist include but not limited to the following:
	  • Evaluate and/or selection of wireless equipment
	  • Advice on any blind spots that affect the wireless signal
	  • Site survey
	• Prepare for installation of wireless LAN
	  • Identify the location of wireless router/Access Point and can be connected to the wired local network or to Internet service provider
	  • Verify power availability for the wireless router
	  • Verify Access Point (AP) has mounting space and signal are not obstructed that reduced transmission efficiency
	  • Acquired network settings
	  • All required equipment have been checked, verified working, and installation manuals are available
	• Install and configure the wireless router
	• Perform a wireless coverage test. Install wireless extension device to increase network coverage and remove blind spots, if needed
	• Configure security settings that conform to the network design and the organisation security policies
	• Install and configure wireless LAN cards on personal computers or join mobile client and smartphone to the wireless LAN then perform the following tests:
	  • Test connection of the wireless network with user equipment to ensure general compatibility and access
	  • Perform speed tests to ensure client connection is of expected performance
	  • Perform security tests to ensure only authorised clients can connect to the wireless network
	• Label all wireless LAN equipment in accordance with the designed infrastructure plan/diagram
	• Provide instructions sessions and/or tutoring to users on use of wireless network, topics include:
	  • Pairing with designated Service Set Identifier (SSID)

	• Logon arrangements • Use of wireless LAN equipment • Document all installation activities and record configuration and security settings details in accordance with the organisation's guidelines and procedures 3. Exhibit professionalism • All installation activities and preparation of documents were performed in accordance with organisation guidelines and standards • Always protect the organisation against unauthorised wireless connection and apply industry network security best practices • Follow the organisation's occupational health and safety guidelines and procedures when installing with network equipment
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Perform the necessary preparations before the installation of wireless LAN • Install, configure and test the wireless LAN and equipment in accordance with the organisation's requirements and standards • Provide sufficient and satisfactory training to users that enable them to access the organisation network resources
Remark	

Specification of Competency Standards for ICT Operation and Support

Unit of Competency

Functional Area: Network Support

Title	Install and configure network components/devices
Code	107880L2
Range	This unit of competency applies to support personnel who install and configure network components or devices in a small internal Local Area Network (LAN) environment. A small network would comprise of Internet connection with wireless and wired Internetworking devices such as switches, routers, wireless LAN Access Points (AP).
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for installing and configuring network components/devices:
	• Possess basic network troubleshooting skills
	• Possess good knowledge of system and network monitoring equipment
	• Possess good knowledge of internetworking devices
	• Possess good knowledge of network concepts, such as:
	  • Network types
	  • Types of cables and distance limits
	  • Wireless LAN
	• Possess good knowledge of the TCP/IP protocol
	• Possess basic knowledge of procedures for handling electrical devices
	2. Installing and configuring network components/devices
	• Comprehend the installation requirements including:
	  • Types of network component/device
	  • Verify location is suitable for the installation work
	• Prepare for installation work
	  • Assess network component/device power and cabling needs
	  • Verify location is suitable for the installation
	  • Acquire the network component/device
	  • Acquire technical manuals and comprehend the installation and configuration instructions
	  • Acquire network configuration information for the network component/device
	• Perform the installation of network component/device complying to the organisation and manufacturer's procedures
	• Configure and test the network component/device to ensure it complies with the organisation's network requirement
	• Clean installation site and return equipment to appropriate location
	• Document the installation and configuration according to the organisation guidelines and standards
	3. Exhibit professionalism
	• Adhere to the organsiation's occupational safety procedure
	• Well converse with industry's networking best practices

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Be well prepared for the installation work • Follow the work order and install the network component/device according to the manufacturer and the organisation procedures • Perform post installation procedures satisfactorily and well document the configuration details and installation work according to the organisation standard procedures
Remark	

Specification of Competency Standards for ICT Operation and Support

Unit of Competency

Functional Area: Network Support

Title	Install and configure client/server application
Code	107882L3
Range	This unit of competency applies to support personnel who install and configure client/server application at workplace. The installation may be for a fresh deployment of the organisation wide client/server application or re-installation when client/server application is having issues. The type of client/server application this UoC refers to is of “tightly coupled” type like POS (Point Of Sales) systems rather than “loosly coupled” type like web browser to web server (any). Also it is installed in an internal network.
Level	3
Credit	6

Competency	Performance Requirements
	1. Knowledge for installing and configuring client/server application
	• Possess basic literacy skills to comprehend work orders and technical documents
	• Possess basic knowledge of networking concept
	• Possess good knowledge of client and server concept in particular
	• Possess good knowledge of common operating systems (server and client)
	• Possess good knowledge of testing and troubleshooting client/server applications
	2. Install and configure client/server application
	• Develop installation plan for the client/server application requirements including but not limited to the following:
	  • Identify what installation options are required from work order
	  • Identify hardware requirement (i.e. server and client side)
	  • Identify software requirement (i.e. database, middle ware, etc.)
	  • Identify network requirements
	  • Identify security requirements
	  • Identify what data migration is required, if any
	• Preparing for installation
	  • Upgrade hardware of server and client device, if required
	  • Acquire the client/server application installation media
	  • Familiarised with the client/server application installation instructions from vendor documents
	  • Acquire associated settings for the client/server application, such as:
	  • IP address of the server and client
	  • Network settings
	  • Authorised access account settings
	  • Acquire all necessary technical manuals
	  • Backup the server and client systems
	  • Install and configure network protocol, middleware, database, if required
	• Install and configure the server side of the client/server application as required by the work order
	  • Configure security and access settings to allow client to connect
	  • Undertake restore or migration of data, if required
	  • Perform appropriate tests
	• Install and configure client side of the client/server application as required by the work order
	  • Configure security setting to enable access to the server side
	  • Configure appropriate functions of the application
	  • Perform tests to ensure client side is forming as required
	• Perform post installation procedures
	  • Clean up work area and remove temporary work files and objects from the server and client device

	• Perform backup image of the server and client for system restore, when and if required • Return and store installation media in secure place as instructed by the organisation's guideline • Document the installation and configuration according to the organisation guidelines and standards 3. Exhibit professionalism • Adhere to the organisation's occupational safety procedure • Well converse with industry's best work practices for installing client/server applications
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Perform the pre-installation activities and being well prepared to ensure the installation of the client/server application without any delay • Ensure the installation process was carried out efficiently without affecting other applications and/or services on the server and clients side • Perform post installation procedures that complied with the organisation guidelines and procedures
Remark	

Specification of Competency Standards for ICT Operation and Support

Unit of Competency

Functional Area: Network Support

Title	Configure WAN connection
Code	107883L3
Range	This unit of competency applies to IT support personnel who are responsible to configure the organisation's internal network to connect and communicate with the external Wide Area Network (WAN) or be connected to the Internet. The configuration will involve configuring the organisation's routers as well of internal hosts. Hosts in this UoC can be user client devices (PCs, mobile devices, tablets, wireless APs, etc.) or servers.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for configuring WAN connection: • Possess good literacy skills to interpret network diagram/plan, technical documents, equipment manuals and specifications • Possess basic network installation and configuration skills • Possess good knowledge of internetworking devices • Possess detailed knowledge of the TCP/IP protocol • Possess good problem solving skill • Possess basic knowledge of organisation guideline and safety procedures for handling electrical devices 2. Configure WAN connection • Prepare the readiness of the internal network to connect with the WAN, including the following: • Comprehend the organisation network plan and architecture, including: • Number of internal subnets • Routing settings of each subnet • De-Militarised Zone (DMZ) information • Load balancing for multi WAN connections • Acquire and install router as per required by manufacturer • Acquire internal network settings from network administrator and configure into the router • Liaise with WAN service provider to confirm switch-over date and WAN connection to be installed • Determine connection type (static IP or DHCP assigned) and configure with reference to the organisation's network plan. For static IP address connection to the WAN, acquire the network setting from service provider • Configure and test router with the given WAN IP address • Test the internal and external connection to ensure traffic can flow on both directions • Configure and test host connections • Document the installation and configuration details according to the organisation guideline and standards 3. Exhibit professionalism • Adhere to the organisation's occupational safety procedure • Well converse with industry's networking best practices

Unit of Competency

Functional Area: Network Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Liaise with WAN service providers to coordinate the cabling and installation of WAN modems into the premises that conform to the network diagram/plan • Configure and test router connection with the WAN connection • Configure all hosts of the internal network to enable them to communicate via the WAN connection
Remark	

Unit of Competency

Functional Area: Network Support

Title	Troubleshoot network issues
Code	107884L3
Range	This unit of competency applies to junior IT personnel who are involved with troubleshooting network issues while in a network supporting role. These junior IT personnel is expected to troubleshoot operational wireless and wired network problems, such as device connection issues, software configuration issues, and network component failure issues. For this UoC devices could be: personal computers, notebooks, tablets, smartphones, internetworking components such as routers, switches, etc.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge to troubleshoot network issues: • Possess good communication and interpersonal skills • Possess good network troubleshooting skills • Possess basic knowledge of different network technologies • Have good understanding of network components and their functions • Possess good knowledge of how to acquire technical information from manuals, colleagues and Internet • Possess good knowledge in operating network testing equipment

Unit of Competency

Functional Area: Network Support

Competency	2. Troubleshooting network issues
	• Acquire details of network issues from problem reports or by communicating with users to understand symptoms of network issues
	• Attempt to reproduce the network issues on user's client device or network component, if possible
	• For wired network connection issues
	  • Inspect for loose cabling on the network devices, network clients, and network components. Reconnect and secure cables
	  • Use cable testing equipment to test cable to ensure it is still functioning
	• For wireless connection issues
	  • Determine where the issues lie, at wireless client or Access Point side
	  • Verify the wireless access point is functioning using other devices or clients
	  • Verify the wireless connection setting and the correct password is used at the client side
	• For software configuration issues
	  • Acquire network settings from network administrator
	  • Verify the software configuration setting matched the network settings. Reconfigure if necessary
	• For network component issues
	  • Verify the device is receiving power
	  • Perform visual check if power cable is connected
	  • Verify power adapter of the device is working and securely connected
	  • Verify the device's power is on
	  • Verify the device configuration setting is correct
	  • Verify the device is transmitting and receiving signals
	• Document all troubleshooting activities and record all findings. Also complete problem report in accordance with the organisation's guidelines and procedures
	3. Exhibit professionalism
	• All troubleshooting activities and preparation of documents were performed in accordance with organisation guidelines and standards
	• Follow the organisation's occupational health and safety guidelines and procedures when working with network equipment

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Prepare sufficiently for the troubleshooting job • Systematically perform troubleshoot tasks and find the network issues • Follow procedures and be able to prepare documents and complete problem reporting in accordance with organisation standard
Remark	

Unit of Competency

Functional Area: Security Support

Title	Create and maintain user accounts on server
Code	107885L2
Range	This unit of competency applies to support personnel who administer the organisation's servers. A very important task for the administrator or the support personnel of servers is to create accounts of users that are allowed to access the system's resource. This UoC assumes servers are standalone and not in directory service environment
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge for creating and maintaining user accounts on server • Possess system troubleshooting skills • Possess good knowledge of system logs • Possess good knowledge of common server operating systems • Possess good knowledge of operating system's access control • Possess basic knowledge of information security • Possess knowledge of the organisation's user security procedures and guidelines

Unit of Competency

Functional Area: Security Support

Competency	2. Create and maintain user accounts on server
	• Determine the needs of the accounts on server, such as:
	  • The role of the user (user, administrator, operator, etc.)
	  • Which server, if there are more than one
	  • Personal folder for the user
	  • Access to server resources
	  • Application settings
	  • Access rights
	• Login to server with administrative account to create the new account and follow the organisation guidelines to setup security settings for the account based on the role of the user. Settings include but not limited to the following:
	  • Security role of the account
	  • Directory and file permissions
	  • Password length
	  • Change password requirements and duration
	• Set temporary password and set user must-change-password on first login
	• Inform the user of new account details
	• Regularly use system tools or third party tools to determine security and usage of accounts, such as but not limited to the following:
	  • Accounts involved with unusual activities
	  • Attempt to access unauthorised resources
	  • Accounts locked out
	  • Unused accounts
	• Handle unusual account activities in accordance to the organisation guideline, such as escalating to supervisor
	• Verify unused accounts and follow the organisation procedures to perform clean-up activities, such as remove account, revoke permission, etc.
	• Document and record all actions performed on user account in accordance with the organisation guidelines
	3. Exhibit professionalism
	• Apply system administrator ethics and exercise due diligence when administering user accounts on servers
	• Exhibit security attitude but balance the needs of users with the organisation security needs when administering system user accounts, as well as securing the server

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand the needs for creating new accounts • Use appropriate system tools to create accounts, perform correct configurations, setup correct access rights to server resources and provide sufficient details and guidance to user that enabling him/her to access the server • Monitor account usage and account irregular activities and take corrective actions to maintain accounts current and secured on the server
Remark	

Unit of Competency

Functional Area: Security Support

Title	Configure user access control on server
Code	107886L3
Range	This unit of competency applies to support personnel who administer the organisation's servers. To access resources on a server the user will need appropriate access rights which administrator will need to configure. Access control in modern servers has pre-configured access control in form of different roles or via traditional access rights.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for configuring user access control on server
	• Possess system troubleshooting skills
	• Possess good knowledge of system logs
	• Possess good knowledge of common server operating systems
	• Possess good knowledge of operating system's access control
	• Possess basic knowledge of information security
	• Possess knowledge of the organisation's user security procedures and guidelines
	2. Configure user access control on server
	• Determine what role the user is allocated by the organisation, for example:
	  • Administrator
	  • Backup operator
	  • Application administrator
	  • Read only analyst
	• Use server management tools to assign the role to the user's account
	• Determine resource access permitted for the user, such as but not limited to the following:
	  • Local logon
	  • Internet access
	  • Remote logon
	• Use server tool to configure user accounts with allowed access
	• Create a check list of access control setting for each shared resources and/or object, such as but not limited to the following:
	  • Printers
	  • Folders
	  • Files
	  • Applications
	• Configure the allowed access and level of access (Read, Write, Execute, etc.) to each object and shared resource
	• Document and record all user access setting and configuration for reference
	3. Exhibit professionalism
	• Comply system administrator ethics and exercise due diligence when administering user accounts and access control on servers
	• Exhibit security attitude but balance the needs of users with the organisation security needs when setting user access control as well as protecting the server

Unit of Competency

Functional Area: Security Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Determine and setup the role of the user that matches his/her access on the server • Identify all the individual objects, shared resources on the server which the user requires access to • Setup and configure correctly the user's access control on the server
Remark	

Specification of Competency Standards for ICT Operation and Support

Unit of Competency

Functional Area: Security Support

Title	Administer system security
Code	107888L3
Range	This unit of competency applies to support personnel who administer the organisation's system security on client devices. The duties of support personnel includes installing various security applications, performing various system configuration and setting to protect the system from loss of information (user and organisation) and different network security risks. Client devices mainly refer to personal computers, notebooks and business tablets
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for administering system security
	• Possess good communication and interpersonal skills
	• Possess system troubleshooting skills
	• Possess good knowledge of system and network logs
	• Possess good knowledge of common operating systems
	• Possess broad knowledge on functions and features of network devices
	• Understand network security and system security risks
	• Possess knowledge of the organisation's security procedures and guidelines
	2. Administer system security
	• Comprehend the organisation's system security requirements and system security plan, including but not limited to the following:
	  • List of authorised personnel/users that can access the system
	  • Level of access/tiered access, or what each user is allowed and not allowed to do on the system
	  • Access control methods, or how users will access the system (user ID/password, digital card, biometrics)
	  • System setting and application needed to strengthen the system and how weaknesses are handled
	  • Which system required system backup and what type of backup procedure to apply
	  • Network security settings and configurations
	• Install the required security application, such as:
	  • Antivirus and spyware protection applications
	  • Personal firewall
	  • Malware protect application
	• Configure and set remote access and support function according to the organisation guideline and procedure
	• Configure network and firewal
	• according to the organisation's guideline
	• Create and setup user accounts in accordance with organisation security requirements
	• Review files security settings and modify access and read/write permissions to match user's role.
	• Regularly perform backups, system security checks, system updates
	• Monitor and record security checks
	• Document and record details of installed applications, configurations, settings, risks for system audit, maintenance and support purpose
	3. Exhibit professionalism
	• Exhibit security attitude but balance the need of users with the organisation security need when administering system security

Unit of Competency

Functional Area: Security Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comprehend the system security plan • Install the required security applications, correctly configure and perform appropriate setting that complied with the security plan • Perform scheduled system security checks, system update and document system changes in accordance with the organisation's guidelines and procedures
Remark	

Unit of Competency

Functional Area: Security Support

Title	Strengthen workstation protection
Code	107891L3
Range	This unit of competency applies to support personnel who are responsible for securing client workstation. Workstations are vulnerable to local and external threats, they need to be protected from as much as these threats as possible. Most organisation will have different protection procedures which support personnel need to setup before allowing user to access the workstation. This UoC illustrates some of the protection tasks and it is by no means exhaustive.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for strengthening workstation protection • Possess system troubleshooting skills • Possess detailed knowledge of security features and functions of the organisation's operating systems • Possess good knowledge of system security concepts • Possess good knowledge of computer hardware and system software • Possess knowledge of the organisation's security procedures and guidelines

Unit of Competency

Functional Area: Security Support

Competency	2. Strengthen workstation protection
	• Comprehend the organisation's guideline for workstations protection to configure the user's workstation. Systematically setup and configure protection features on the workstation
	• Setup physical security protection, including but not limited to the following:
	  • Lock the CPU unit to prevent opening of the case
	  • Affix a chain lock (Kensington lock) to secure position for notebooks
	• Setup password protection (hardware-level) for access to machine's BIOS
	• Eliminate or disable unnecessary services. For example: remote access, Internet sharing, etc.
	• Remove unnecessary executables and registry entries to prevent attacker invoking disabled programs
	• Set user account to
	  • "non-administrator" account, to prevent uncontrolled change of system settings
	  • Avoid multi-user sharing same machine, if possible
	• Set system account policies
	  • Minimum length of account password
	  • Force change password
	  • Set re-used policy
	• Setup screen save to turn off screen and power off system after a predefined period of no user activities
	• For systems holding confidential information, setup file encryption and access permission
	• Install and setup anti-virus, anti-spyware and anti-malware scanning and handling, such as:
	  • Auto and scheduled update of virus definitions
	  • Scheduled daily scan
	  • Real time protection
	  • Anti-virus application which starts on system boot
	  • When virus or malware found, clean first (high risk) and quarantine second
	• Setup firewall protections
	• Setup auto and scheduled system updates
	• Create a backup image of the workstation before allowing user to use the machine
	• Document the system settings and configurations for internal record
	3. Exhibit professionalism
	• Exhibit security ethics and balance the need of users with the organisation security needs when setting and configuring security protection of user's workstations

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comprehend the organisation's workstation protection guidelines and able to configure and setup required security protections • Complete documents of the security settings and configuration in accordance with the organisation's procedures
Remark	

Unit of Competency

Functional Area: System and Hardware Support

Title	Provide support to mobile device users
Code	107904L3
Range	This unit of competency applies to IT support personnel who are responsible for mobile device support to users. As organisations are joining the Bring Your Own Device (BYOD) bandwagon, users will need supporting in the work environment; IT support staff will need to have the necessary skills to support and educate users using mobile devices to access the organisation resources. This UoC concerned on area of general support including but not limited to: setup brand new devices to access organisation resources, assist logon and use of Mobile Device Management (MDM) system, protection of corporate information in event of loss of mobile devices, remote support access and support, change configuration and settings, etc.
Level	3
Credit	6
Competency	Performance Requirements 1. Knowledge to perform remote support: • Possess good communication, listening and interpersonal skills • Possess remote support skills capable to perform troubleshooting, provide instructions systematically and remote problem solving • Possess good knowledge of functions and features of the organisation’s MDM system • Possess good knowledge of mobile device supported applications • Possess good knowledge of common mobile device platforms such as IOS, Android, Blackberry, Windows Phone, etc. • Well conversed with the organisation’s BYOD guidelines and procedures • Possess good knowledge of virtual desktop technology and Virtual Desktop Infrastructure (VDI) for mobile device

Unit of Competency

Functional Area: System and Hardware Support

Competency	2. Perform remote support
	• Listen attentively and patiently to understand the user's reported issues
	• Refer to the Trouble Ticket System (TTS)/problem reporting system to determine if similar issues and/or solutions exist
	• For brand new BYOD mobile devices, follow the organisation guidelines to perform some but not limited to the following tasks:
	  • Ensure user understand, agree and accept the organisation policies, particularly when device is misplaced/lost
	  • Install organisation MDM apps and organisation's standard apps
	  • Install mobile support apps, such as: Teamviewer for mobile, Remoty, GotoAssist, etc.
	  • Configure network access setting such as VPN
	  • Backup device
	  • Turn on remote wipe function of the device
	  • Install anti-virus/malware/spyware app
	  • Create new access accounts on MDM server and test connectivity and accessibility to ensure device is function as expected
	• For troubleshooting or remote support, mobile support application or MDM apps should be used to remote access to the mobile device, to view and change setting, screen capture, direct communicating with user to provide instructions to resolve the issue
	• For misplaced/lost device, evaluate the risk of data loss and assist the user to use "find my phone/device/mobile" function or use MDM apps to trace, lock or wipe the device
	• Provide instructions and/or training to users on mobile devices usage and mobile security to protect organisation data
	• Create a new or update Trouble Ticket (TT)/problem report to record the activities transacted during the support session
	3. Exhibit professionalism
	• Possess customer service oriented attitude
	• Apply industry best practices for mobile support and being up-to-date with mobile technology trends

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Set up the users' mobile devices to conform with the organisation's mobile device policies • Use appropriate tools to troubleshoot mobile devices, resolve users experience issues and assist or advice users with correct solutions to resolve issues for providing effective support to users and protect the organisation data in the event of user loss • Take correct actions to protect the organsiation's data in the event where users have lost mobile devices • Provide sufficient instruction or training to users on use of mobile devices that conform with the organisation policy
Remark	

Unit of Competency

Functional Area: System and Hardware Support

Title	Troubleshoot client device hardware issues
Code	107905L3
Range	This unit of competency applies to IT support personnel who are responsible for providing support for client devices. Client devices ranging from personal computer to smart mobile device could experience hardware issues during its operation and support personnel are requested to fix the issues. This UoC concerns the identification of hardware issues before it can be fixed.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for troubleshooting client device hardware issues
	• Possess good troubleshooting and problem analysis skills
	• Possess good knowledge of operating client devices
	• Possess good literacy skills for reading technical manuals of client devices
	• Possess good knowledge of the organisation's procedures for troubleshooting client devices
	• Possess basic knowledge of hardware protection procedures, such as use anti-static straps, etc.
	• Possess basic knowledge of the organisation health and safety guideline
	2. Troubleshoot client device hardware issues
	• Comprehend symptoms, if any, prior issues appeared from problem report and/or discussion with user. For example:
	  • Nothing came on when power button pressed
	  • Blank screen but CPU unit appears to be running
	  • System running very slow and continuously rebooting or hanged
	  • System not responding to mouse and keyboard
	• Review maintenance records of the device, to determine if maintenance work has contributed or caused the issues
	• Prepare for troubleshooting:
	  • Acquire all necessary technical and user manuals
	  • Acquire tools to open the client device and tools for troubleshooting
	  • Acquire device components or spare parts
	• Analyse and formulate a troubleshooting plan
	• Without opening to inspect the inside of the client device, perform checks for loose connections, power sockets, battery, display device, etc.
	• View the BIOS error message display code or listen for the number beeps sounded and verify the given code with technical manuals to identify BIOS detected error. For example:
	  • 1 = Loose memory module
	  • 2 = CPU error repair/replace mother board
	  • 3 = display memory error repair/replace display card
	• Next stage of checking is to verify connected components have not affected the functioning of client device, such as:
	  • Keyboards/mouse (swap with a known working component)
	  • Battery low power on mobile device (swap with a fully charged battery)
	  • Hard disk failure (listen for unusual noise)
	  • Power supply unit failure (verify cooling fan is functioning and/or system light is on)
	• For intermittent issues, such as "system hang" or "randomly rebooting" under heavy system work load, identify cause of issue using combination of techniques, including but not limited to the following:
	  • System log messages
	  • Reproduce the issues with monitoring tools
	  • Incorrect BIOS settings

	• Overheating components • Purpose-built hardware analysis device • For mobile device, once verified it is not battery problem and still cannot be started, return the devices to vendor who will use manufacture's hardware problem analysis devices to identify the issues • Once the cause of issues have been identified, formulate a rectification action plan and clean the work area • Document and record the findings in accordance with the organisation procedures and standards 3. Exhibit professionalism • Follow organisation safety guidelines and procedures when performing troubleshooting of client devices
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Prepare well with troubleshooting work, having all the required tools and manuals for use during the troubleshooting process • Plan the troubleshoot work and systematically perform the troubleshooting to identify the issues or cause of issues • Follow the organisation safety procedures during the troubleshooting process
Remark	

Unit of Competency

Functional Area: System and Hardware Support

Title	Perform remote support
Code	107907L3
Range	This unit of competency applies to support personnel who are responsible for providing remote support. In a structure support team this would be a Level 2 support personnel where Level 2 is normally the first point of escalation, provides guidance and instructions to Level 1. Level2 is where the support personnel take ownership of incidents where subject matter expertise and experience is required for diagnosis. However, this UoC concerned only remote support competencies and does not distinguish the organization level.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge to perform remote support: • Possess good communication and interpersonal skills • Possess remote support skills capable of performing troubleshooting and providing systematic instructions for remote problem solving • Possess good knowledge and operating remote support applications • Understand committed Service Level Agreement (SLA) and standards • Possess good knowledge of problem escalation procedures and guidelines • Possess basic knowledge of the organisation computer hardware, Operating System (OS), applications and network equipment

Unit of Competency

Functional Area: System and Hardware Support

Competency	2. Performing remote support
	• Comprehend reported problem from Trouble Ticket system (TTS)/problem report system to understand symptoms and diagnostics from support desk colleague (level 1 support)
	• Search TTS/problem report system to determine if similar issues and/or solutions exist
	• Communicate with the customers/users to explain actions that will be performed to resolve the issue, such as:
	  • Need to collect more information related to the reported issue
	  • Need to remote access to user's system
	  • Will instruct the user to self-rectify the issue upon determination that the user is capable of self-rectification
	• If remote access/control is necessary, determine customer/user's comfort level to have remote access feature of the system turn on and installation of remote access software. To gain customer/user's support it is necessary to explain:
	  • How the remote access work compare with on-premise support
	  • There are no security risks
	  • Benefits of remote access/control
	• Perform troubleshoot and/or apply solution to correct the reported issue. If remote solution cannot fix the issue then offer to customer/user the on-premise support option
	• Confirm solution is acceptable with customer/user
	• Uninstall any application and/or reset configurations that were used for the remote support purpose and remind users to set off remote support functions on their system
	• Document all activities and record changed setting in the TTS/problem report. Where necessary, coordinate with other colleagues, such as requesting on-premise engineers to visit the customers/users
	3. Exhibit professionalism
	• Possess customer service oriented attitude
	• Always keep customer informed of actions and status of the rectification process
	• Follow industry best practices to use best remote support application to provide remote support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comprehend the reported problem from the internal TTS/problem report system and able to update the appropriate record in accordance with the organisation's procedures after the completion of the remote support session • Persuade customers/users to allow remote access/control to their system for troubleshooting and/or correcting of issues • Perform the remote support to the satisfaction of customers/users
Remark	

Unit of Competency

Functional Area: Web Support

Title	Troubleshoot web browser and connection issues
Code	107909L3
Range	This unit of competency applies to support personnel who are responsible for providing front line support on web browser usage to users on different client platforms, including desktops, notebooks, tablets and even smartphones. The web browser is one of the most used applications. Very often users will encounter many issues which will need assistance. Common issues encountered including but not limited to the following: cannot start browser, wrong security setting, incompatibility, malware, connection problem, unable to initiate download after click of links, etc. To assist users the support personnel will troubleshoot and provide a remedy. Additionally the support personnel should provide some basic tutorial to users to avoid repetition and facilitate self-help.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for troubleshooting web browser and connection issues: • Possess good communication and interpersonal skills • Possess good troubleshooting skills and capable of providing systematic instructions for remote problem solving • Possess good knowledge of functions of various web browsers on different platforms • Possess basic knowledge of operating different computing platforms • Possess basic knowledge of web browser development and trends such as: technologies, web browser features, malwares attacks, etc. • Possess basic knowledge of the organisation’s network infrastructure

Unit of Competency

Functional Area: Web Support

Competency	2. Troubleshoot web browser and connection issues
	• Patiently listen to user describing issues and symptoms. Use appropriate questioning techniques to gather as much information to help troubleshoot the issue:
	  • What are the types of issue user is experiencing,
	  • What type of browser
	  • What platform and OS environment the browser is operating on
	• Refer to history problem log to determine if similar problems and solutions exist
	• If web browser shows “cannot connect to server” or similar message, then troubleshoot network connection by verifying and correcting below items:
	  • Verify the client is actually connected to the network (LAN or mobile)
	  • Verify client has acquired a valid IP and DNS address
	  • Verify correct proxy server setting
	  • etc.
	• If displayed content is inconsistent with the new contents of the web site, then clear the cache of the browser
	• If downloads are not permitted or no activities after user clicked a link, then review and adjust the security settings that prevent certain risky functions and scripts from auto activated, such as: ActiveX, cookies and downloads. Any adjustment of security setting must be complied with the organisation security policies
	• If web browser cannot start then locate related error messages from system or application logs to determine the issue. If application is corrupted, and no alternative method of correcting the problem, then uninstall and reinstall the Web browser
	• If the browser consistently redirected to unwanted web site, this may be due to the browser being hijacked by malware. Use anti-malware software to detect and remove the malware
	• Explain the cause of issues and remedies applied to users and provide some basic training and advice to user on “best practices on using web browser and surfing internet”
	• Create or update problem log in accordance with the organisation’s procedures and issues and remedies performed
	3. Exhibit professionalism
	• Possess customer service attitude with desire to assist users with problems
	• Follow organisation safety guidelines and procedures when troubleshooting and/or reification of equipment

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Systematically apply web browser troubleshooting techniques to identify the cause of issues and provide remedies • Use correct level of technical language to gather information related to the Web browser issues and conduct tutorial to users • Complete the “after event” procedures in accordance with the organisation’s standards
Remark	

Specification of Competency Standards for ICT Operation and Support

Unit of Competency

Functional Area: Web Support

Title	Maintain website performance
Code	107910L3
Range	This unit of competency applies to IT support personnel who are responsible to maintain the performance of the organisation's website. One of the tasks of website maintenance is to ensure the site is running at an optimal speed that can provide a good user experience to visitors and a successful website with business.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for Maintain website performance
	• Possess good knowledge of various website performance testing tools, such as : Webpage analyser, Google's site tool and Google Page Speed, Yahoo's YSlow, etc.
	• Possess good knowledge of creating web contents
	• Possess basic knowledge of different web browsers
	• Possess good knowledge of the organisation basic network infrastructure
	• Possess good knowledge of the organisation website performance requirements
	2. Maintain website performance
	• Work with supervisor and/or colleagues to identify the website response time required. Different types of responses for different types of contents
	• Verify the website performance using suitable performance testing/measuring tools
	• Study the website network and hosting server performance
	  • If loading is high, consider off load some of the tasks from the server
	  • If web server is hosted on a Cloud Server, consider using a different hosting service provider
	• Work with content developers to review and advice on some but not limited to the following:
	  • Minimise size of webpage
	  • Minimise the use of nested table
	  • Avoid using oversized image file straight from camera. Resize image files to a match the purpose
	  • Optimise programs, scripts and databases
	• Regularly run stress tests to ensure the performance of the website is within the organisation's standard
	• Document performance test results for reporting purpose
	3. Exhibit professionalism
	• Possess quality of service attitude. Website performance affects the organisation image and business

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Work with supervisors or colleagues to identify the and formulate a performance standard for the organisation's website • Use performance measuring tools to determine the performance of the organisation website • Work with website developers to improve performance of the website to meet the organisation's performance requirement
Remark	

Unit of Competency

Functional Area: Web Support

Title	Build simple web site using content management systems
Code	107911L3
Range	This unit of competency applies to IT personnel who are responsible for building a simple web site for the organisation. Most companies will want to have an Internet presence; having at least a simple web site and IT personnel are entrusted with building this web site. As Internet and web content management system (CMS) technologies are maturing, building web sites is almost as simple as creating “Office” documents. However, once the web site is built the IT personnel will need to provide tutorials to webpage designer on use of CMS editor to build webpages. This UoC assumes the web site is hosted by hosting service provider.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for building simple web site using content management systems
	• Possess good communication and interpersonal skills
	• Possess good knowledge of web hosting concept and sourcing of hosting facilities
	• Possess detail knowledge of implementing web CMS systems
	• Possess detail knowledge of operating and administering the organisation’s CMS
	• Possess basic knowledge of HTML
	• Possess some basic training skills
	2. Build simple web site using content management systems
	• Work with supervisor and other stakeholders to identify the website technical requirements from, such as:
	  • Type and usage of web site (dynamic, static, Internet store, etc.)
	  • Performance required (response time)
	  • Size of storage
	  • Network speed
	• Identify suitable web CMS and web hosting company (unless for the organisation use, taking into various factors, including:
	  • Prices
	  • Backup service
	  • Facilities offered (storage, network bandwidth, CPU speed, etc.)
	• Prepare purchasing document, in accordance with organisation procurement procedures, and recommendation for supervisor approval
	• Liaise with hosting service provider to setup DNS reference to the organisation’s new web site and acquire hosting servers logon details to administer the CMS
	• Download and perform remote installation web CMS on hosting server
	• Access administrative functions of web CMS to perform following tasks:
	  • Upload and install a template for the website
	  • Upload company logo and other media (pictures and video) contents for the home page
	  • Edit the home page with CMS editor
	• Test the web site with different web browsers to ensure compatibility
	• Create login accounts and provide tutorial sessions for web designers to use the CMS editor to create web pages on the web site
	3. Exhibit professionalism
	• Be familiar with W3C web standards and ensure the CMS and web site are W3C compliant
	• Always look after the interest of the organisation when dealing with external parties

Unit of Competency

Functional Area: Web Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Fully comprehend the requirements of the type of web site the organisation is building and acquire sufficient technical details to subscribe to a web hosting service • Install the CMS on the hosting server and be able to use the CMS editing tools to create the web site's home page that is compatible with common web browsers • Provide sufficient tutorial and assistance to web page designers that enable them to construct other web pages without any difficulties
Remark	

Unit of Competency

Functional Area: Web Support

Title	Maintain website
Code	107912L3
Range	This unit of competency applies to IT personnel who are responsible to maintain the organisation's website. The website is the window of companies to the Internet world. It represents the organisation. Hence, it is essential to be always in operation and the contents are update without any embarrassing issues, such as customer cannot complete purchasing transaction or students cannot upload (hand in) projects or homework. This UoC concerned with the website maintenance of the content rather than the physical server which the website is hosted on.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for maintaining website: • Possess interpersonal and coordination skills • Possess basic knowledge of principles of website design and maintenance • Possess good knowledge of creating web contents • Possess basic knowledge of operating common web browsers • Possess good knowledge of operating website testing tools • Understand user feedbacks or complaints related to the website • Understand the organisation's website performance requirements • Possess basic knowledge of the organisation document standards and procedures

Unit of Competency

Functional Area: Web Support

Competency	2. Maintain website
	• Coordinate with various parties in the organisation to implement new features, upload new contents to website
	• Create various channels to receive information related to the organisation's website, included but not limited to the following:
	  • Visitor feedbacks or user complaints
	  • Results of website testing tools
	  • Monitoring/log statistics
	  • Alerts of website outage
	• Periodically perform tests including but not limited to the following:
	  • Access to the website is still possible
	  • Web contents are compatible with different browsers and different clients (mobiles and desktops)
	  • No broken links
	  • Software are updated
	  • Access and download speed
	  • Functions/features are operational as expected, such as: checkout, blog, forum, registration, upload, download, etc.
	• Correct or coordinate with appropriate parties to correct any detected issues and remove redundant contents
	• Collect visitor traffic statistic for security purpose and/or business use
	  • Pages entered on and exited on
	  • Time spent on the site
	  • Bounce rate
	  • Referring sites
	  • Countries of visitors are from
	• Use monitoring tools for "Reputation management" of the organisation's name, brands and contents of the website appeared on the Internet, such as Google alert
	• Apply backup strategies:
	  • Perform scheduled backups
	  • Perform drills for recovery, in the event of website corruption
	• Document and create reports that comply with the organisation's standards and procedures for assisting website developers and management decision making
	3. Exhibit professionalism
	• Look after the interest and reputation of the organisation
	• Apply industry best practices and web technologies when maintaining website
	• Adhere to Intellectual Properties and copyright laws

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Use different tools to monitor and test organisation's website • Liaise with appropriate parties to correct issues and ensure the website is fully functional, updated and tested with different browsers on different clients • Ensure the website is well backup according to the organisation's planned schedules and can be recovered within the organisation standard
Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Perform installation, configuration and testing of network equipment and devices
2. Code	111106L3
3. Range	This UoC concerns initial installation, checkout and enablement of continuous operation of network equipment and devices at the end user's site. The installation of equipment and devices may need connecting to the "Access Network" or enabling communicating effectively with other network equipment. Equipment's include broadband modem, optical line terminal (OLT), optical network unit (ONU) / optical network terminal (ONT), router, switch, wireless equipment, voice telecom equipment (PABX/Keyline, etc.), VOIP equipment, IoT gateways, sensors and actuators, etc.
4. Level	4
5. Credit	6 (For Reference Only)
6. Competency	Performance Requirements 6.1 Possess the knowledge in the subject area ● Be able to: ■ Comprehend and follow "Work Order" requirements and schedules ■ Follow equipment and/or IoT devices installation instructions from supervisor ■ Comprehend product/equipment/device manuals ■ Comprehend site plan/drawings, wiring diagrams, equipment and/or device drawings, etc. ■ Possess experience in network cabling/equipment/device installation ■ Be able to conduct mechanical and electronic preventative maintenance to predict problems & correct anomalies ■ Apply basic network principles or protocols knowledge for simple device configuration, like IP address setup in network devices ■ Operate troubleshooting tools including personal computer and its operating system, RF monitors, cable testers, etc. ■ Understand the basic functions of the testing tools ■ Communicate effectively with customers to understand network or equipment problems and able to give work progress/status so as to maximise customer satisfaction 6.2 Perform installation, configuration and testing of network equipment and devices ● Be able to:

	■ Verify work order with customers and confirm an installation appointment ■ Gather and prepare equipment/devices for installation ■ On arrival at the premises, communicate with customers to understand the network issues and provide a brief description of the job nature ■ Use site plans/drawings to locate local connection (TNT – Telecom Network Termination) /interface to Access Network (ETP- External Terminating Point)/Lead-in cable, if needed. ■ Install any local transmission media (e.g. 2 wire, UTP, coaxial, wireless), if necessary and CPE. Perform tests to ensure correct termination ■ Install local network equipment (including broadband or other transceiver such as DSL, modem, VOIP, etc.) and/or IoT edge devices (including sensors and actuators). DSL splitting at DTP (Disconnect Test Point) may be required ■ Connect local network equipment and/or IoT devices to telecommunication outlets ■ Determine the correct power supply for the network equipment and/or IoT devices such as power of ethernet (POE) ■ Install appropriate software and perform necessary configuration settings, such as IP address, if applicable ■ Perform the tests to determine working order of the installed equipment and/or devices ■ Fill in “Work Order” completion form and communicate with customer to ensure customer is satisfied with the work and request “Work Order” to be signed off 6.3 Exhibit professionalism ● Be able to: ■ Communicate with customers in a professional manner and keep customers updated of work status ■ Follow safety procedures at every step of installation procedure ■ Ensure equipment and/or devices are installed to required quality standard and conformed to the organisation and international standards
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● communicate effectively with client/customer or supervisor to understand and verify work orders ● prepare the network equipment and/or IoT devices for installation according to work order ● install, configure and test the network equipment and devices to required job order and manufacturer specification ● perform tests according to the job order specification ● complete the necessary documentation and ensure the installation

	job is satisfactorily signed off
8. Remark	Equipment/devices installation can be performed in-house or at customer site. Hence, soft skills in dealing with customer are essential for troubleshooting and keeping customer informed of job status.

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

Functional Area – (IoT)

1. Title	Perform network testing
2. Code	111107L4
3. Range	This UoC defines the competency required for performing network performance and/or capacity tests which include telephone network, Personal Area Network (PAN), Local Area Network (LAN), Wide Area Network (WAN) / Low Power Wide Area Network (LPWAN), Metropolitan Area Network (MAN), wireless (Mobile or WiFi) or wireline, etc.
4. Level	4
5. Credit	3 (For Reference Only)
6. Competency	Performance Requirements 6.1 Possess the knowledge in the subject area ● Be able to: ■ Possess extensive experience in test planning, and testing procedures and analysis of test results or statistics from testing equipment ■ Able to comprehend and follow test plans, network infrastructure diagrams and configuration setting specifications ■ Possess extensive experience with network performance analysis, defining metrics for testing of networks and network components. ■ Experienced with network optimisation techniques such as queuing theory, routing, switching and transmission optimisation. ■ Possess extensive experience with using testing tools and setting up testing environments ■ Knowledgeable of health and safety rules and hazards related to the equipment and/or tools being used during testing 6.2 Perform network testing ● Be able to: ■ Comprehend the network testing requirements from test plans and test procedures of test cases ■ Plan and setup test environments. Define test baselines and specify how to collect evidence of test cases ■ Perform the test cases as per the test plan and collect test results with evidence like: logs, monitoring reports, network equipment configurations ■ Analyse results and compare with baseline to determine: ◆ Any incorrect testing procedure – in such case correct or change testing methods or procedures ◆ Network performing normally

	◆ Network performing poorly ■ Document the testing procedures, setups, and results, conforming to the organisation standard and summaries the results, with any particular actions required and/or any particular areas to be noted ■ Present the testing results to stakeholders for action or decision making 6.3 Exhibit professionalism ● Be able to: ■ Follow safety procedures at every step during the setup and while performing testing ■ Ensure all documentations are carried out in accordance with the organisation's policies and standards
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● follow test plan, design the testing procedures, setup test environments and carryout network testing systematically in accordance with the test case requirements ● document the whole testing scenario, results and any observations, in accordance with the organisation documentation standards
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Perform Installation and configuration of internet server application
2. Code	111120L4
3. Range	This UoC involves carrying out installation and configuration of internet server application according to predefined requirements.
4. Level	4
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Knowledge in installation and configuration of internet server application, including ● networking and internet server ● common operating systems ● testing and troubleshooting internet server applications 6.2 Install and configure internet server application ● Prepare an installation plan for the internet server application requirements including but not limited to the following: ■ Identify what installation options are required from work order ■ Identify hardware, software, network and security requirements ■ Identify what data migration is required, if any ● Prepare for installation ■ acquire the server application installation media ■ familiarise with the server application installation instructions from vendor documents ■ acquire associated settings for the server application such as network confgiruations, firewall confgiruations, authorised access account settings ■ acquire all necessary technical manuals ■ perform server backup if necessary ■ install and configure network settings, middleware, database, if required ● Install and configure the server as required by the work order ■ configure security and access settings to allow client to connect ■ apply appropriate patches and updates ■ undertake restore or migration of data, if required ■ perform appropriate tests ● Perform post installation procedures ■ clean up work area and remove temporary work files and objects from the server ■ perform backup image of the server for system restore, when

	and if required ■ return and store installation media in secure place as instructed by the organisation's guideline ■ document the installation and configuration according to the organisation guidelines and standards 6.3 Exhibit professionalism ● perform post installation procedures that in compliance with the organisation guidelines and procedure ● make reference to the industry best practices for installing server applications
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● perform the pre-installation activities and being well prepared to ensure the installation of the server application without any delay ● ensure the installation process is carried out efficiently without affecting other applications and/or services on the server ● perform post installation procedures that complied with the organisation guidelines and procedure
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Apply diagnostic and troubleshooting skills to solve hardware, software and networking related issues
2. Code	111121L4
3. Range	This UoC involves troubleshooting and identifying the causes of the problem in ICT systems.
4. Level	4
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Knowledge in hardware, software and networking aspects and diagnosis of hardware, software and networking aspects in ICT systems. 6.2 Troubleshooting across hardware, software and networking aspects in ICT systems ● comprehend the issues and symptoms of the issues from the problem report or from user and plan how to troubleshoot the issues. ● apply appropriate diagnostic tools and command set to obtain the status of the system. ● attempt to reproduce the issues that were reported and collect as much information as possible for problem analysis. ● When needed, consult colleagues, professionals and vendors ● formulate an action plan to implement the solutions to rectify the issues. 6.3 Exhibit professionalism ● take necessary measures to prevent or minimise data loss or service interruption during the diagnosis process. ● follow organisation safety procedures when handling any hardware or equipment during the troubleshooting process. ● follow organisation Standard Operating Procedures (SOPs) or guidelines when handling the troubleshooting process.
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● apply proper diagnostic tools and system functions for problem identification. ● plan the troubleshoot work and systematically perform the troubleshooting to identify the issues or cause of issues. ● follow organisation procedures when handling any hardware or equipment during the troubleshooting process.
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Define data governance policies and architecture principles
2. Code	111123L6
3. Range	This UoC involves defining the data governance policies and scope of data assets for the establishment of data architecture to support the development of organisational data being accurate, accessible, consistent and protected.
4. Level	6
5. Credit	3
6. Competency	Performance Requirements 6.1 Understand the data governance policies and scope of data throughout the data lifecycle ● Be able to: ■ Have knowledge of data governance policies (see Remark 1) and scope of data (see Remark 2) 6.2 Define the data governance policy for the establishment of data architecture to support the development of organisational data being accurate, accessible, consistent and protected ● Be able to: ■ define the processes to be implemented in your data governance initiative ■ define roles and assign responsibilities ■ initialize the data governance framework ■ define the required deliverables and organization structure for data governance 6.3 Review the data governance policy ● review the data governance policy such that the data asset are consistent and confident for the business decisions based on trustworthy data aligned with all the various purposes within the enterprise
7. Assessment Criteria	● The integrated outcome requirement of this UoC is the abilities to define the governance policy to make consistent and confident business decisions based on trustworthy data aligned with all the various purposes for the use of the data assets within the enterprise
8. Remark	1. The data governance policy will deal with the internal policies and external policies for data quality, access, security, privacy and usage, as well as roles and responsibilities for implementing those policies and monitoring compliance with them against organisational culture, types of business, ethics, regulatory, compliances, standards, etc. 2. The appropriate protection and security levels for different classifications of data within the scopes of data include (but not limited

	to) data ownerships, data custodians, data retention, data sharing, data archive and data disposal

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Determine technology mix for the design and development of embedded software systems
2. Code	111126L6
3. Range	Based on the adopted embedded software architecture model(s), standards, tools and other resources, choose the most appropriate combination of technology mix to design and develop a given embedded software system
4. Level	6
5. Credit	3
6. Competency	Performance Requirements 6.1 Comprehend different embedded software architecture models and the technologies (See Remark 1) behind them ● Be able to: ■ formulate different combinations of the adopted embedded software architecture model for a given embedded software system to be developed for the organisation ■ review and recommend a particular combination of the adopted embedded software architecture models (including its design, patterns, variants, and various supporting technologies) for a given embedded software system 6.2 Select and recommend the most appropriate technology mix for the adopted embedded software architecture model ● Be able to: ■ review various technology mixes (combinations of technology) ■ perform comparison and trade-offs analysis among various technology mixes (See Remark 2) ■ propose the most appropriate technology mix to design and develop a given embedded software system based on the adopted embedded software architecture model 6.3 Choose the most appropriate technology combination to design and develop a given embedded software system based on the adopted embedded software architecture model in a professional manner ● review, select and recommend the most appropriate technology combination to design and develop a given embedded software system based on the adopted embedded software architecture model ● ensure that the most appropriate combination supports good software design and development practices, and are in compliance with organisation's guidelines as well as any local and international

	laws and regulatory requirements, where applicable
7. Assessment Criteria	The integrated outcome requirement of this UoC is the ability to select and recommend the most appropriate technology mix (combination) for the design and development of a given embedded software system based on the adopted embedded software architecture model.
8. Remark	1. Examples of various technologies of embedded software framework and platforms are Embedded Linux, WebOS, Android, Desktop Linux/Windows, QNX. Integrity, VxWorks, Ubuntu and Debian, Windows for IoT, Embedded Configurable Operating System (eCos), etc. 2. This may involve performing trade-off analysis on an implementation of a given system function through software, hardware and/or the most optimal combination of both. 3. Pre-requisite: ITSWAR619A 4. Co-requisite: ITSWAR621A

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Define metrics to ensure that a technology architecture meets the business goals
2. Code	111127L5
3. Range	Define metrics to evaluate and analyse technology architectures to ensure that it can support the business goals and objectives.
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the principles of quality assurance ● articulate the needs for quality assurance to ensure that the resulting technology architecture really meets the required quality standards ● understand the quality assurance standards and measures provided by IT service providers 6.2 Understand the purposes of relevant metrics for quality assurance standards ● understand appropriate and measurable metrics to evaluate the ability of a technology architecture to meet the business goals and objectives (See Remark) 6.3 Define metrics for quality assurance standards ● keep updated of the business and technology changes ● observe the code of practices in trade ● update the developed software deployment or migration plan and contingency plan whenever necessary 6.4 Exhibit professional skills ● a formal checkpoint review of the architecture model and building blocks with stakeholders, validating that the business goals are met ● document all findings
7. Assessment Criteria	The integrated outcome requirements of this UoC is the ability to: ● validate that the business goals and other objectives of implementing the technology architecture are met. Please note that this may be a continuous exercise because of the ongoing changes of business requirements and technology options. This makes the definition of quality assurance standards and metrics a key to this activity.
8. Remark	An example of the metrics can be a key question list which is used to pose questions against the architecture model and service description

	portfolio to test its merit and completeness

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Analyse the performance, latency and accessibility of systems
2. Code	111130L4
3. Range	This UoC involves analysing the performance, latency and accessibility of computer systems across multiple processing environment in accordance with the organisation's guidelines and/or requirements.
4. Level	4
5. Credit	3 (For Reference Only)
6. Competency	Performance Requirements 6.1 Understand the attributes to measure the performance of computer systems across multiple processing environment, including but not limited to: ● Availability ● Extensibility ● Interoperability ● Maintainability ● Reliability 6.2 Understand the effect of latency and accessibility of computer systems across multiple processing environment, including but not limited to: ● Virtualization ● Distributed computing ● Data center Location ● Sensor and actuator network ● Streaming media ● Esports and online multiplayer games 6.3 Know the enhancement of accessibility and analyse the performance of computer systems across multiple processing environment to provide suitable strategies for the benefits of the organisation
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● analyse the performance, latency and accessibility of computer systems across multiple processing environment for an organisation in accordance with its guidelines and/or requirements. ● provide suitable recommendations for the benefits of the organisation.
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Develop and perform data acquisition and collection processes and conduct pre-processing and exploratory data analysis
2. Code	111131L5
3. Range	This Uoc involves conducting data acquisition processes including hack/wrangle complex data, selecting appropriate techniques relevant to the problem. Utilising a range of data audit techniques and approaches for data quality assessment and data quality verification. Conducting data cleaning of noisy, incomplete data or data with data quality issues
4. Level	5
5. Credit	3 (For Reference Only)
6. Competency	Performance Requirements 6.1 Have knowledge of data acquisition and collection processes and pre-processing and exploratory data analysis ● Be able to: ■ have knowledge of data acquisition and collection processes (See Remark 1) ■ have knowledge of pre-processing and exploratory data analysis (See Remark 2) 6.2 Appraise and manage different data acquisition methods ● Be able to use appropriate methods to acquire data from internal or external sources 6.3 Conduct pre-processing and transformation of the data ● Be able to conduct pre-processing and transformation of the data to ensure that it is in the optimal format, layout or shape for the project purposes using feature engineering or exploratory data analysis 6.4 Conduct and review data quality processes ● Be able to conduct and review data quality assessment for missing values, duplicates, multiple sources and inconsistent formats
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● have knowledge of data acquisition and collection processes and pre-processing and exploratory data analysis; and ● develop and perform data acquisition and collection processes and conduct pre-processing and exploratory data analysis to obtain the data being valid, accurately interpreted, and applicable to the desired contexts
8. Remark	1. Various Data Acquisition Methods are collecting new data; converting/transforming legacy data; sharing/exchanging data; and

	purchasing data. This includes automated collection (e.g., of sensor-derived data), the manual recording of empirical observations, and obtaining existing data from other sources. 2. Exploratory data analysis (EDA) is a term for certain kinds of initial analysis and findings done with data sets, usually early on in an analytical process. Pre-processing of the data will be performed by analysing the data either categorical or numerical, visualizing them and some statistical decision.

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Design customised data management tools and services to manage the target data for an organisation
2. Code	111142L6
3. Range	This Uoc involves designing and developing data management tools and services that are not available from the existing markets to manage the target data based on different requirements including capacity, performance, reliability, recoverability, discovery scheme, etc.
4. Level	6
5. Credit	6 (For Reference Only)
6. Competency	Performance Requirements 6.1 Understand the practices of data management throughout its lifetime through the internal (and external) data streams of an enterprise ● know the data management being a comprehensive set of concepts, procedures, practices, processes, and a number of systems that allow for an organization to gain control of the data assets ● know the data operations covered in data management (See Remark 1) ● know the requirements of using different data management tools/services/platforms (See Remark 2) ● know the differences among in-house, outsourced and hybrid development of data management tools/services/platforms 6.2 Design and develop the right data management tools/services/platforms to fill the gap between the data management requirements and the data management tools/services/platforms from existing markets ● select the appropriate design and development tools/environments for building the targeted data management tools/services/platform ● design and develop the right data management tools/services/platforms to fill the gap between the data management requirements and the outsourced data management tools/services/platforms from existing markets ● test the developed data management tools/services/platforms 6.3 Evaluate the developed data management tools/services/platforms with the integration of existing ones based on the use of the data
7. Assessment Criteria	The integrated outcome requirement of this UoCs are the abilities to: ● design and develop the right data management tools and services that are not available from the existing markets to perform the necessary data management processes to meet the data requirements for the organisation

	● evaluate the developed data management tools/services/platforms with the integration of existing ones based on the data objectives
8. Remark	1. Data management covers the following operations (but not limited to): - create, access, and update data across diverse data tiers - store data across clouds and on-premise - use data across applications, analytics, and algorithms - provide high-availability and disaster recovery - secure data and provide privacy - archive and destroy data based on retention rules and compliance requirements. 2. The requirements of using different data management tools and services include (but not limited to) capacity, performance, reliability, recoverability, discovery scheme, security, etc.

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Design customised analytics and modeling tools for an organisation
2. Code	111147L6
3. Range	This UoC involves designing and developing the customised data analytics solutions and/or modelling tools (if ready-made solutions/tools are not sufficient) by applying different technologies (such as ML and AI techniques) for an organisation.
4. Level	6
5. Credit	3 (For Reference Only)
6. Competency	Performance Requirements 6.1 Understand the practices of data analytics processes, data analytics solutions and/or modelling tools throughout its lifetime through the internal (and external) data streams of an enterprise ● know the data analytics solutions and/or modelling tools/processes being a comprehensive set of concepts, procedures, practices, processes, and a number of systems that allow for an organization to analyse the data ● know a wide range of core data science/analytics techniques, their advantages, disadvantages and areas of application in different dimensions (See Remark 1) ● know different analytics technologies (See Remark 2) ● know the necessity of the data analytics and data models, relevant objectives, time and resource requirements 6.2 Plan and develop the right data analytics solutions and/or modelling tools/processes to fill the gap between the data analytics/models requirements and the data analytics solutions and/or modelling tools/processes from existing markets ● select the appropriate design and development programming tools, languages and environments (See Remark 3) for building the targeted data analytics solutions and/or modelling tools/processes ● design and develop the right data analytics solutions and/or modelling tools/processes to fill the gap between the data analytics/models requirements and the outsourced data analytics solutions and/or modelling tools/processes from existing markets ● test the developed data analytics solutions and/or modelling tools/processes 6.3 Evaluate the developed data analytics solutions and/or modelling tools/processes with the integration of existing ones based on the data objectives
7. Assessment	The integrated outcome requirement of this UoC are the abilities to:

Criteria	● design and develop the right data analytics solutions and data model using the right data analytics solutions and/or modelling tools/processes which are not available from the existing markets in order to meet the data requirements for the organisation ● Evaluate the developed data analytics solutions and/or modelling tools/processes with the integration of existing ones based on the data objectives
8. Remark	1. Data dimensions: - traditional vs. emerging data - structured vs. unstructured data 2. The analytics technologies include (but not limited to) statistical methods, data mining methods, machine learning, deep learning, reinforcement learning through various AI techniques 3. The programming languages/platforms include (but not limited to) R, Python, Anaconda, IDLE, Jupyter Notebook, Spyder, etc.

Specification of Competency Standards
for the Information and Communications Technology Industry
Unit of Competency

1. Title	Define a system migration plan
2. Code	111155L6
3. Range	Define a system migration plan taking into account the business operations (including contingency plan) in the context of migrating systems
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the requirements in system migration ● Be able to ■ comprehend the organisational requirements, limitations and constraints on the system migration ■ identify all components of the system that need to be migrated ■ know the regulatory requirement such as audit trails or other compliance requirements ■ know the share responsibility model with IT service providers 6.2 Develop and define a system migration plan and a contingency plan ● Be able to ■ perform reviews of software requirements, hardware infrastructure, software architecture, components, interfaces and performance model ■ identify components that need to be updated ■ make suggestions on how to upgrade the system, for example, with the use of the latest technological developments ■ future-proofing the system by accounting for the adaptation of potential future technologies ■ list out the required deliverables upon migration ■ identify the critical success milestone and criteria in migration ■ formulate a system migration plan by integrating the known factors and also taking into account the available migration timeline ■ suggest an alternative contingency plan as a backup to cope with adverse cases ■ alert of associated personnel for potential downtime to minimise impact to the operation of the organisation 6.3 Update the migration plan ● Be able to

	■ stay on top to keep abreast of the pace of business and technology changes ■ observe the code of practices in trade ■ update the developed system migration plan and contingency plan whenever necessary 6.4 Define system migration plan in a professional manner ● Be able to ■ define a system migration plan ■ define the contingency plan of the migration exercise ■ minimise impact to the organisation's operation ■ comply with the organisation's guidelines and procedures as well as any (local and international) laws and regulatory requirements, if applicable
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● devise and update a system migration plan and the related contingency plan for the migration exercise ● minimise impact to the organisation's operation
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Perform system testing against user, technical and hosting requirements
2. Code	111160L4
3. Range	Identify all elements of the system that need to be tested against user and system requirements, including data that should be used to fully test the system.
4. Level	4
5. Credit	3 (For Reference Only)
6. Competency	Performance Requirements 6.1 Have the knowledge to design and develop test plans and software/sensor simulator to facilitate different levels of testing ● Be able to: ■ identify the requirements of test plans ■ identify the requirements of software/sensor simulator, if applicable 6.2 Perform various levels of testing, which may involve the use of a software/sensor simulator ● Be able to: ■ design and develop software/sensor simulator, if applicable, to facilitate different levels of testing ■ perform the required testing activities of various levels of testing according to the corresponding test plans 6.3 Perform all testing activities in a professional manner ● Be able to ■ perform the testing activities of various levels of testing in an efficient and effective manner ■ ensure that all such testing activities are complied with the corresponding test plans and are in accordance with the organisation's guidelines as well as any (local and international) laws and regulatory requirements, if applicable
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● develop appropriate software/sensor simulators, if necessary, for testing purposes; ● perform various levels of testing; and ● document all testing activities in test reports.
8. Remark	Various levels of testing include unit testing, integration testing, system testing – functional testing and performance testing, and user-acceptance testing.

Specification of Competency Standards
for the Information and Communications Technology Industry
Unit of Competency

1. Title	Define user requirements
2. Code	111162L4
3. Range	This UoC involves defining user requirements of IT application and communicating with stakeholders to produce a user requirement document
4. Level	4
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Know the stakeholders and information needed to be conveyed ● understand the relationship of business requirements, user requirements and system requirements for defining an IT application development project ● identify the stakeholders who will be the users of the IT application to be developed ● collect profile of stakeholders, whenever possible, to preliminarily identify what the users do with the IT application or what activities the users must be able to perform ● understand any constraints on the delivery of information such as time and location etc. 6.2 Consolidate information for delivery ● collect relevant data and compose a draft appropriate to the communication assignment ● explain the use of special terms and short forms ● bridge the gap between technical and non-technical people by communicating technical terms in generic terms ● seek recommendation or approval from management before release of information where necessary 6.3 Exhibit professionalism in the user requirement document ● follow the organisation's style and format to prepare the user requirement document ● produce accurate and concise the user requirement document
7. Assessment Criteria	The integrated outcome requirement of this UoC are the abilities to： ● understand and identify the needs of stakeholders for an IT application design project ● communicate technical information to non-technical people effectively ● Produce accurate and concise user requirement document
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Develop procedures to implement incident response plan
2. Code	111170L5
3. Range	This UoC involves designing the process to implement the incident response plan while minimising the impact on the organisation's operation
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand incident response plans ● Understand the processes and operations of the incident response unit ● Aware of the potential scale of incidents and personnel that could potentially be involved ● Understand the tasks that are needed to carry out to have the plan implemented ● Understand the organisation's cyber security policies and assets/infrastructures that could be involved (e.g. Internet of Things, Cloud storage, networks etc.…) 6.2 Develop procedures and guidelines to implement incident response plan ● Determine the responsibility of all associated personnel ● Determine the scale of the tasks that needed to carry out ● Decide the order of the tasks needed to carry out to minimise any interruption to the organisation's operation ● Communicate with relevant departments to understand their needs such that the execution could be planned accordingly to minimise the impact on the organisation's operation ● Ensure that tools and equipment needed for the implementation are all identified and have a plan to make them available for the tasks ● If downtime of essential services are unavoidable, potential backup services should be considered 6.3 Exhibit professionalism ● Comply with the organisation's guidelines and procedures as well as any (local and international) laws and regulatory requirements, if applicable

7. Assessment Criteria	The integrated requirements of this UoC is the ability to design the procedure to implement incident response plan such that impact on the organisation's operation could be minimised
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Evaluate the results of application security assessment for improvement recommendation
2. Code	111173L5
3. Range	Evaluate the results of application security assessment and propose possible directions for security improvement.
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Knowledge of the requirements of application security assessment ● understand the basic principles, methodologies and tools in the application security assessment process (e.g. RASP, MAST) ● appreciate the objectives of the security assessment ● understand the requirements and goals of the security assessment of the organization 6.2 Evaluate the results of application security assessment ● any security weaknesses and vulnerabilities in source code ● any security weaknesses in architecture, design, open source and third-party components ● consolidate the impacts from possible application security risks in qualitative and quantitative terms ● properly document the evaluation results 6.3 Propose possible directions for improvement ● develop a structured plan to coordinate security improvements in according to the organization's guidelines and requirements ● propose best practices for security assessment ● develp training programmes for internal staff to upgrade their competency
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● critically evaluate the results of application security assessment ● propose possible directions for security improvement in according to the organization's guidelines and requirements
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Conduct solicitation planning
2. Code	111197L5
3. Range	This UoC involves preparing and specifying tender details for an organisation to outsource a particular project (whole or some of its part)
4. Level	5
5. Credit	3
6. Competency	Performance Requirements 6.1 Have knowledge in the market condition ● Be able to collect information about the products and services available in the marketplace 6.2 Understand the procurement cycle for outsourcing a particular project (whole or some of its part) ● Be able to understand the outsourcing activities for a procurement cycle 6.3 Prepare complete procurement documents ● Be able to: ■ design structured procurement documents that are used to solicit proposals from prospective sellers such as ◆ invitation for Bid (IFB) ◆ request for Proposal (RFP) ◆ request for Quotation (RFQ) ◆ initiation for Negotiation ◆ contractor Initial Response ■ ensure the documents can facilitate accurate and complete responses from prospective sellers as well as rigorous enough to ensure consistent, comparable but flexible responses to allow sellers to make suggestions for better ways in achieving the requirements 6.4 Be able to define evaluation criteria for rating or scoring proposals including the bidders' ● background ● financial capability ● past track record ● technical knowledge/skill ● resources availability 6.5 Form a tender board ● Be able to formulate the tender board with suitable members for

	the tender evaluation process
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● develop effective procurement documents for the tender bidders submitting bid/quotation; and ● set up an accurate evaluation process for rating and scoring the submitted bids.
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Analyse the available solutions from IT service providers
2. Code	111199L4
3. Range	This UoC involves analysing solutions from external IT service providers that fit most to the organisation's business goals
4. Level	4
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Knowledge in evaluation criteria of external IT service providers ● Technical expertise ● Domain expertise ● Business maturity Evaluation criteria of external IT service providers can also be divided into various sub-criteria. (See Remark 1) 6.2 Rank the proposals according to the criteria as listed in the procurement management plan 6.3 Make preparation for drafting the service agreement with the successful bidder ● Apply appropriate methods to identify service agreement concerns: ■ project warranties ■ liabilities ■ indemnity ■ insurance clause-related activities ● Make negotiation with the external service providers according to the rank sequence ● clarify any unclear points in the received proposal from the external service providers and negotiate with them on the terms and conditions according to relevant local / international laws ● reach consensus on the structure and requirements of the service agreement with the successful bidder prior to the signing of the agreement (Remark 2)
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● apply appropriate criteria to evaluate proposals from external IT service providers ● make a fair selection for a successfully bidder and reach consensus with the successful bidder on the important terms and conditions for drafting the service agreement.
8. Remark	1. The evaluation sub-criteria are: ● Service / Product Value Creation / Provision ■ Service / Product Portfolio: Service scope including the

	completeness of the portfolio or the skill set. ■ Service / Product Experience: Service availability and service experience from a customer perspective. Maturity of the offer. ■ Integration: Interoperability of Technologies with one another or the skills to integrate them. ■ Economic factors: Price transparency and the quality of the business model, not the prices themselves. For service providers, nearshore concepts or skills that deliver low-cost architectures have also been evaluated. ■ Disruption potential: Recognition of the availability of highly innovative approaches ● Vendor Performance ■ Strategy: Strategy and market understanding. Does technology fit the company strategy? ■ Footprint: Competitive strength and market presence in terms of customers, reach, visibility and go-to-market. ■ Ecosystem: For IT service providers, the number of development service providers who are familiar with their technologies is critical. On the other hand, we evaluate the number of technology suppliers that are listed by Development Service Providers under Partners and Skills. Active involvement in open source communities is also a plus. ■ Customer Experience: Availability of information and training for technology providers. Local availability of employees for service providers. ■ Agility: Speed and innovation strength of the providers, assessed in terms of their ability to grasp market trends quickly and, if necessary, develop them with an innovation budget. 2. Subjects covered generally include, but not limited to, responsibilities and authorities, applicable terms and law, technical and business management approaches, contract financing and price.

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Prepare system operation documentation
2. Code	111200L4
3. Range	Prepare technical and user documentation describing how the system works for third party management. Documentation should reflect maintenance and update processes to ensure integrity the deployment.
4. Level	4
5. Credit	3 (For Reference Only)
6. Competency	Performance Requirements 6.1 Understand system requirements ● Be able to: ■ identify system operation issues, i.e. system installation/update and deployment, day-to-day technical operations, server or software application failure and maintenance, etc. ■ comprehend the workflow as stated in the system operation plan according to technical and user requirements 6.2 Prepare the operation documentation containing information that will aid system administrators to understand the functions and capabilities of your information technology systems, applications, and components ● Be able to: ■ describe the user typical processes and operation procedures as required by the needs of the technical and user requirements ■ provide standards on document to help with consistency and avoid potential pitfalls 6.3 Check the consistence and completeness of the documentation ● Be able to: ■ comply with corporate policy in documentation standards ■ review developed templates and guidelines to ensure their consistence in format and their completeness meet with system requirements ■ issue the developed templates and guidelines to stakeholders for review and feedback ■ incorporate feedback from stakeholders and management to finalise the system documentation standards
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● establish system report and documentation standard and ensure consistency and completeness in the operation documentation ● enhance efficiency of system operation, support, maintenance and system training, etc.

8. Remark	

Specification of Competency Standards
for the Information and Communications Technology Industry
Unit of Competency

1. Title	Formulate business strategies and policies
2. Code	111201L6
3. Range	Formulate the business strategies and policies for an organisation in alignment with its approved vision and mission statements by considering the potential impacts and implications of both current and emerging technologies
4. Level	6
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand business objectives and envisioned future of an organisation ● Be able to ■ articulate the core values and purpose of an organisation ■ articulate the current trends of business and the envisioned future of an organisation 6.2 Understand issues related to both business and IT perspectives of the industry ● Be able to ■ understand the issues related to both business and IT perspectives of the industry ■ have insights of technology trends and viability of technology products under market forces ■ understand the potential impacts and implications of current and new technologies in the fields related to the organisation ■ think of possible ways to utilise new technologies in the organisation operation and marking strategy. 6.3 Understand the current development trends of a business ● Be able to summarise the business trends related to the organisation ● Aware of the business profile and positioning of the organisation ● Understand and state up to date with the business field related to the organisation 6.4 Understand the ICT applications related to a business ● Be able to summarise the ICT applications related to the operational aspect of the organisation ● Consider and make suggestions on updating current or adopting new technologies to enhance the operation and governance aspect of the organisation

	6.5 Analyse the strengths, weaknesses, opportunities and threats (SWOT) of an organisation ● Be able to perform a SWOT analysis for an organisation to develop business strategies and policies that bring reasonable and acceptable return of investment (ROI) 6.6 Formulate strategies and policies for the sustainability of the business ● Be able to ■ formulate the strategies and policies for the long-term sustainability of the business taking into consideration Business-IT alignment and enablement ■ formulate partnership/alliance strategies with external partners like vendors/suppliers, investors, distributors to win the market ■ carry out the above in accordance with the organisation's business goals, objectives, policies and guidelines as well as any (local and international) laws and regulatory requirements, where applicable 6.7 Formulate ideas where IT can help the growth of the business ● Be able to identify and think of ways to update and implement technologies that could strengthen the operational goal and governance of the organisation
7. Assessment Criteria	The integrated requirements of this UoC are the abilities to： ● formulate business strategies and policies for an organisation in alignment with its approved vision and mission statements to support its sustainable development ● suggest updates to current technologies and adaptation of new technologies that could assist the development and governance of the organisation
8. Remark	Some examples of emerging ICT technologies are: ● Artificial intelligence and machine learning ● Cloud computing ● Internet of things ● Security and automation

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Identify and evaluate information technologies that support the objectives of an organisation
2. Code	111202L6
3. Range	This UoC involves applying analysis methods to identify and evaluate the information technologies that fit most to the organisation's business processes
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the organisation's objectives ● comprehend the organisation's vision, mission, objectives, goals and plans ● seek clarification on the above from relevant people, if necessary ● understand the implications of the organisation's objectives on the application of emerging technologies 6.2 Have broad knowledge of the information technologies applicable to the organisation's industry ● understand the emerging technologies landscape, including but not limited to: ■ Artificial intelligence and machine learning ■ Cloud computing ■ Internet of things ■ Security and automation ● understand the applicability, advantages and disadvantages, constraints and limitations of various information technologies available for the specific industry of the organization ● evaluate the opportunities and threats of the emerging technologies ● Understand the shared responsibility model with IT service providers, if applicable 6.3 Identify and evaluate information technologies that support the organisation's objectives with a high degree of expertise and professionalism ● identify and evaluate the appropriate information technologies for the organisation using standard guidelines and methodologies ● consider and evaluate the appropriateness of managed or outsourcing services. ● make appropriate references to industry sources, such as vendors

	and their customers, experts and consultants in the industry, etc.
7. Assessment Criteria	The integrated outcome requirement of this UoC is the ability to ensure that the information technologies identified and evaluated are the most appropriate to support the organisation’s objectives.
8. Remark	

Specification of Competency Standards
for the Information and Communications Technology Industry
Unit of Competency

1. Title	Review and comply with organisational policies and procedures, relevant laws and regulatory requirements
2. Code	111205L6
3. Range	This UoC involves reviewing practices to ensure that the service delivered adhere to the organisational policies and procedures, relevant laws and regulatory requirements
4. Level	6
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Have knowledge of organisational practices, infrastructures, policies and procedures ● know the operational structure of the organisation ● aware of the different technologies, tools, equipment and online services that are related to the service or tasks delivered ● understand the organisation's policies, procedures and goals ● observe organisational practices and procedures 6.2 Have knowledge of relevant laws and regulatory requirements related to the industry of the organisation ● comprehend the latest regulatory requirements applicable to the organisation, including but not limited to: ■ Intellectual property right protection ■ Personal data (Privacy) ordinance ■ National security law ■ Telecommunications ordinance ● refer to the appropriate experts for guidance where necessary 6.3 Review and comply with organisational policies and procedures, relevant laws and regulatory requirements ● Identify the applicable laws and compliances ● observe and adhere to relevant policies and procedures, laws and regulations in an efficient and effective manner ● take the initiative to improve the organisation's policies and procedures where appropriate ● obtain the endorsement of relevant stakeholders ● obtain prior approvals for system resources and access, such as communication protocols and ports, data storage, online services,

	other system peripherals, computer time as well as data of another person ● review practices, identify and rectify any noncompliance procedures ● make use of tools, infrastructures, equipment and online services available to enhance the service delivered ● make suggestions to enhance existing or purchase of new tools, infrastructures, equipment and online services if it helps to improve on the compliance to related regulations or the effectiveness of the service delivered ● make effective and efficient use of external experts where necessary to meet its business goals and objectives ● report serious misconducts and noncompliance procedures to relevant management and suggest methods to avoid future occurrences (such as provide training programs or workshops to highlight issues to relevant personnel)
7. Assessment Criteria	The integrated requirements of this UoC are the abilities to： ● review of own practices; identify and rectify any noncompliance procedures ● comply to organisational policies and procedures, relevant laws and regulatory requirements ● obtain prior approval for system access and resources according to the aforementioned policies and requirements ● Utilise existing resources and make suggestions on updating or acquiring new resources to enhance the service delivered and adhesion to various related policies and regulations ● Report serious misconducts and noncompliance procedures to relevant management and suggest methods to avoid future occurrences (such as provide training programs or workshops to highlight issues to relevant personnel)
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Set policy to control data security and privacy
2. Code	111206L6
3. Range	Establish policy to control data security and privacy of an organisation
4. Level	6
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand legal requirements on data security and privacy ● locate and make reference to sources of legislation applicable to local business entities (Remark) ● seek professional advices on issues relating to security and privacy 6.2 Observe standards, guidelines and procedures published by professional bodies ● comprehend the standards, guidelines and procedures published by professional bodies in the trade and extract the sections relevant to organisational operation as reference 6.3 Set corporate policy to control data security and privacy ● formulate control policies to cover stages from data capture and processing, information flow and distribution, storage and access to retirement ● formulate control policies to ensure that information is relevant, accurate and timely and its management is an integral part of strategic management ● formulate control policies to maintain confidentiality, integrity, and reliability throughout the stages to comply with administrative, audit and legal requirements 6.4 Keep the policy up to date ● perform regular review on the local and international policies to ensure it meets the changing operational environment ● cross check the policy with current best practice as published by professional bodies in the trade to make optimum use of the information resources 6.5 Set policy to control data security and privacy in a professional manner ● establish the required policies in accordance with organisation's guidelines as well as any (local and international) laws and regulatory requirements, if applicable
7.	The integrated outcome requirements of this UoC is the ability to produce a

Assessment Criteria	policy document addressing the control of data security and privacy.
8. Remark	Some reference sources of legislation applicable to business entities are: ● Bilingual Laws Information System http://www.legislation.gov.hk/eng/index.htm ● Personal Data (Privacy) Ordinance http://www.pcpd.org.hk/english/ordinance/ordfull.html ● General Data Protection Regulation (GDPR) https://gdpr.eu/ ● The Personal Information Protection Law of the Mainland https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html ● The PRC Data Security Law http://www.hk-lawyer.org/content/new-prc-data-security-law-and-its-potential-impact-overseas-data-transfers

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Review the emerging technologies and cross-functional strategies
2. Code	111207L6
3. Range	Review cross-functional strategies to enable an organisation to identify suitable emerging technologies for supporting its business strategies
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand issues associated with emerging technologies ● evaluate the values of the emerging technologies with respect to business-technology alignment and enablement of the organization ● understand the deployment procedures of the emerging technologies ● keep updated of the application development areas of various emerging technologies, including but not limited to: ■ Artificial intelligence and machine learning ■ Cloud computing ■ Internet of things ■ Security and automation ■ Streaming technologies ● aware of the data security and privacy concerns in the domains of various emerging technologies 6.2 Review cross-functional strategies for deploying and managing the emerging technologies ● review the organization business strategies, and conduct a mapping between the possible application areas of emerging technologies with the business strategies ● setup a clear digital strategy, if necessary, to ■ identify the appropriate technology applications for different operations of the organization ■ prioritize projects that require cross-functional collaboration ■ setup the project management team for cross-functional projects
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to ● conduct a mapping between the possible application areas of emerging technologies with the business strategies ● setup digital strategy to support the deployment and management

	of cross-functional projects
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Review the ethical and social issues for IT applications
2. Code	111208L6
3. Range	This UoC involves reviewing/addressing the social, environmental, political and legal challenges related to the emergence and convergence of information and communication technologies from the point of view of morality and ethics.
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the moral and ethical dimensions for IT applications ● identify and understand the major moral and ethical dimensions that tie together ethical, social, and political issues in IT applications including ■ Information rights and obligations ■ Property rights and obligations ■ Accountability and control ■ Application/system quality ■ Culture and lifestyle: economic disparity, equality and ethnicity on rights ● understand the impacts from technology advancement on individual and society such as data collection and analysis, privacy invasion etc. 6.2 Review the ethical and social issues for an organisation ● review the IT applications and/or processes within the organization from the point of view of morality and ethics ● identify and properly record any shortfalls relevant to moral and ethical considerations 6.3 Exhibit Professionalism ● always look after the interest of the organisation as well as customers.
7. Assessment Criteria	The integrated outcome requirements of this UoC is the ability to review the social, environmental, political and legal challenges related to IT applications/systems to support organisation's business strategies from the point of view of morality and ethics
8. Remark	

Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

1. Title	Implementing monitoring equipment to monitor infrastructure failure and security breaches
2. Code	111429L4
3. Range	For a network to operate reliably and efficiently, continuous monitoring is required to detect faults and security breaches so that appropriate actions can be taken. This UoC describes the competencies for implementing monitoring equipment to monitor infrastructure failure and security breaches.
4. Level	4
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Possess the knowledge in the subject area ● Expert in implementing various types of network monitoring management tools, Internet of things (IoT) device management software, alarm management tools, log management, system messages, software systems ● Knowledgeable of the operational requirements, duties, functions, and procedures of network related systems of the organisation ● Extensively experienced with network monitoring and implementation of monitoring equipment ● Possess in depth knowledge of network infrastructure, diagrams, maps and access network plans ● Possess extensive knowledge of the operating characteristics of the network components ● Understand the organisation's security policy 6.2 Implementing monitoring equipment to monitor infrastructure failure and security breaches ● Be able to: ■ Determine from work orders or supervisors the type of monitoring and objective of performing monitoring thresholds e.g. to meet SLA commitment to customers, to collect statistic for capacity planning, for support purpose, etc ■ Identify the appropriate monitoring equipment to use and consider alternatives ■ Determine and define operating baselines for the network infrastructure or components ■ Acquire trigger criteria from appropriate parities (product owners, network engineers, customers) and configure

	triggering network equipment with the required trigger settings. ■ Ensure that triggers record are documented and alerted the associated personnel ■ Set monitoring equipment to monitor the threshold points. The monitoring equipment should produce the required statistics and report for analysis and, if necessary, trigger alarms ■ Perform simulated tests of the monitoring equipment to verify the setting is correct ■ Fully document the implementation steps with network diagrams showing where triggers start, end, monitoring threshold, etc. Extra user procedures will be required for any internally developed monitoring equipment/software ■ Distribute copies of the document to appropriate parties (supervisor, network engineers, etc.) for vetting and filing in accordance with the organisation standards and procedures ■ Demonstrate the completion of the implementation with test results and acquire stakeholders or supervisor signoff ■ Ensure that all tools implemented are secured and complied with the organisation's cybersecurity policy 6.3 Exhibit professionalism ● Follow safety procedures while configuring and implementing network monitoring equipment ● Ensure documents conform to the organisation's standards and policies ● Always take into consideration and strike a proper balance among all related technological, environmental and legal factors
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● identify and fully understand the monitoring requirements from work orders and/or supervisors ● identify the monitoring factors such as trigger points, threshold, and output requirements (logs, alerts, alarms, etc.) ● correctly select the appropriate monitoring equipment to monitor the network functions and/or security of the network infrastructure ● Ensure all tools implemented are secured and complied with the organisation's cybersecurity policy ● successfully implement the monitoring by setting/adjusting/configuring monitoring devices to record statistics, trigger alarm/alert or send messages ● successfully demonstrate the completion of the implementation of the monitoring equipment with test results and documentation

8. Remark	

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Understand key characteristics of embedded software systems	
2. Code	ITSWAR521A	
3. Range	Demonstrate clear understanding of the key characteristics of embedded software systems through the application of suitable principles in the design of such software systems [Architecture – Embedded Software Architecture]	
4. Level	5	
5. Credit	3	
6. Competency		Performance Requirement
	6.1 Understand key characteristics of embedded software systems	Be able to explain key characteristics of embedded software systems and their effects on the design of embedded software systems See Remark 1 for some examples of key characteristics of embedded software systems
	6.2 Understand the overall design requirements of embedded software systems	Be able to explain the overall design requirements of embedded software systems See Remark 2 for some examples of design requirements of embedded software systems
	6.3 Understand the design principles applicable to embedded software systems	Be able to explain the various design principles and how they are applicable to embedded software systems
	6.4 Apply the suitable principles in the design of embedded software systems	Be able to use the suitable design principles in the design of embedded software system
	6.5 Design the embedded software system in a professional way	Be able to demonstrate high degree of professionalism and competence in the design of embedded software systems
7. Assessment Criteria	The integrated outcome requirement of this UoCs is the ability to apply suitable principles professionally in designing embedded software systems.	
Remark	1. Some examples of key characteristics of embedded software systems are a) high dependence on hardware platform; b) small software footprints and code efficiency; c) many are real-time in nature; d) purpose-built for very specific problems; e) high reliability and robustness (self diagnostics and self correction are common requirements); and f) extremely high software quality (as distribution of software corrections after production release can be prohibitively costly). 2. The overall design requirements of embedded system might include: a) purpose of the system; b) input and output specifications; c) performance criteria; d) usage patterns and environment; e) usability requirements and constraints; f) hardware platform; and g) physical constraints and footprint.	

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Manage and maintain the program source	
2. Code	ITSWDM505A	
3. Range	Manage and maintain the program source via proper version control mechanism in the context of development of software products / services within an organisation or for a client [Design, Development and Maintenance – Software Development (Programming) and Related Activities]	
4. Level	5	
5. Credit	2	
6. Competency		<u>Performance Requirement</u>
	6.1 Understand version control mechanism	Be able to understand version control mechanism used by the organisation
	6.2 Manage program source	Be able to ▪ manage the consistency of program source format ▪ manage the storage / backup of program sources
	6.3 Maintain program source	Be able to ▪ maintain program source via proper version control mechanisms ▪ Standardize the numbering systems for version control within the organization
	6.4 Act in line with software configuration management	Be able to ▪ appreciate the change control policy in configuration management ▪ manage and maintain program source with alignment to configuration management activities
7. Assessment Criteria	The integrated outcome requirements of this UoCs is/are the abilities to: (i) manage program source; and (ii) maintain program source via proper version control mechanism.	
Remark	Activities in this competence may intertwine with SCM1-2.	

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Perform inspection for the program code and software documents (See Remark 1 for the meaning of "inspection")	
2. Code	ITSWDM506A	
3. Range	Perform inspection, walkthrough and review for the program code and software documents according to the Quality Assurance (QA) policies in the context of development of software products / services within an organisation or for a client [Design Development Maintenance – Software Quality Assurance]	
4. Level	5	
5. Credit	2	
6. Competency		<u>Performance Requirement</u>
	6.1 Have the knowledge to design checklists for inspecting program source and software documents	Be able to identify the requirements of checklists (see Remark 3 & 4) for inspecting program source and software documents
	6.2 Perform inspection of program source and software documents	Be able to ▪ create checklists for inspecting program source and software documents ▪ inspect the program source and software documents according to the items in the inspection checklist ▪ determine the correctness and quality of program source and software documents after inspection ▪ complete the relevant items in the checklist
	6.3 Revise and update the checklist after an inspection	Be able to revise and update the items in an inspection checklist for future improvements
	6.4 Perform inspection of program source and software documents professionally	Be able to perform an inspection of program source and software documents according to ▪ the QA policies of the software project ▪ the organization's guidelines ▪ any (local and international) laws and regulatory requirements, if applicable
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) rigorously perform inspection of program source and software documents according to the QA policies and procedures according to the developed inspection checklist; and (ii) evaluate the correctness and quality of the program source and software documents after inspection.	
Remark	1. In this UoCs, "inspection" generally means "inspection", "walk-through" and "review" of certain software artefacts such as program source and software documents. 2. In this UoCs, "software document" generally means any document related to the software such as software requirements specification and various software design documents. 3. The inspection checklist should have at least the following categories: a) Architecture Review; b) User Interface; c) Data Reference; d) Data Declaration; e) Computation;	

	f) Comparison; g) Control Flow; h) Input/Output; and i) Interface. 4. The inspection checklist can be checked by another professional/third party.

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Develop test plans for various levels of testing (See Remark for various levels of testing)	
2. Code	ITSWDM507A	
3. Range	Develop test plans for various levels of testing in the context of development of software products / services within an organisation or for a client [Design Development Maintenance – Software Quality Assurance]	
4. Level	5	
5. Credit	2	
6. Competency		<u>Performance Requirement</u>
	6.1 Have the knowledge to design test plans according to the software requirements specification (SRS) and other software documents	Be able to identify the requirements of various level of test plans according to the SRS, various software design documents and program source
	6.2 Develop test plans for various levels of testing	Based on software documentations such as the SRS, various software design documents and program source, be able to ▪ develop test plan for unit testing ▪ develop test plan for integration testing ▪ develop test plan for system testing ▪ develop test plan for functional and performance testing ▪ develop test plan for user-acceptance testing
	6.3 Ensure the total cost for software testing is within budget	Be able to ▪ evaluate the total cost for software testing according to various level test plans ▪ review the test plans if the cost exceeds the budget
	6.4 Develop test plans for various levels of testing in a professional manner	Be able to ▪ develop test plans for various levels of testing ▪ ensure the total cost for testing is within the budget in accordance with the organization's guidelines as well as any (local and international) laws and regulatory requirements, if applicable
7. Assessment Criteria	The integrated outcome requirements of this UoCs is the ability to design effective test plans for various levels of testing.	
Remark	Various levels of testing include unit testing, integration testing, system testing – functional testing and performance testing, and user-acceptance testing.	

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Lead and motivate a team	
2. Code	ITSWGS604A	
3. Range	Lead and motivate a team in the context of managing and leading an organisation [Generic Skills – Management and Leadership – Personal Attribute]	
4. Level	6	
5. Credit	6	
6. Competency		<u>Performance Requirement</u>
	6.1 Have knowledge of the theories and techniques of leading and motivating a team	Be able to ▪ understand the specific and unique needs of a team ▪ understand the various theories and techniques available for leading and motivating a team
	6.2 Apply suitable skills in leading and motivating a team	Be able to ▪ analyse and diagnose the specific and unique needs of a team, referencing appropriate theories and/or methodologies ▪ reference suitable sources to assist in the analysis and diagnosis ▪ steer and align team efforts with organisational objectives ▪ motivate team members to share knowledge and experience
	6.3 Lead and motivate a team with a high degree of expertise and professionalism	Be able to ▪ gain the respect and trust of the team members ▪ adjust leadership and motivational skills to cater to the different situations ▪ encourage full participation in meeting social responsibilities as well as quality performance ▪ lead the team to achieve results to the best of its capabilities and potentials
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) demonstrate effective leadership in a team situation; (ii) motivate the team to a high spirit towards achieving certain goals; and (iii) lead a team to achieve excellent results that are aligned with organizational objectives.	
Remark		

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Delegate responsibilities	
2. Code	ITSWGS606A	
3. Range	Delegate responsibilities in the context of managing and leading an organisation [Generic Skills - Management and Leadership – Personal Attribute]	
4. Level	6	
5. Credit	3	
6. Competency		<u>Performance Requirement</u>
	6.1 Have knowledge of the theories and techniques of delegation	Be able to ▪ understand the specific strengths and weaknesses of each staff ▪ understand the needs for delegation ▪ understand the various theories and techniques available for delegation of responsibilities
	6.2 Apply suitable skills in delegating responsibilities	Be able to ▪ analyse the strengths and weaknesses of staff ▪ delegate responsibilities to staff in accordance to their strengths and abilities ▪ clarify the understanding of staff on their responsibilities
	6.3 Delegate responsibilities to staff with a high degree of expertise and professionalism	Be able to ▪ delegate responsibilities to staff in a clear, effective and unambiguous manner ▪ exploit the full potential of staff in the delegation, and develop staff to the best of their capabilities and potentials ▪ achieve the best synergy among staff in the delegation
7. Assessment Criteria	The integrated outcome requirement of this UoCs are the abilities to (i) delegate responsibilities to suitable staff; (ii) develop staff potentials via proper job / task allocations; and (iii) exploit staff's full potentials via proper job / task allocations.	
Remark		

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Manage changes	
2. Code	ITSWGS613A	
3. Range	Manage changes within the organization [Generic Skills - Change Management]	
4. Level	6	
5. Credit	5	
6. Competency		Performance Requirement
	6.1 Understand change	Be able to ▪ understand the importance and need for changes ▪ understand the implications of changes
	6.2 Cope with changes positively	Be able to ▪ identify if a change has occurred ▪ evaluate the impacts resulting from the change ▪ manage the change ▪ document the change
	6.3 Grasp opportunities for improvement	Be able to ▪ minimize negative impacts resulting from the change ▪ leverage on the change to enjoy positive outcomes which would not have been obtained if the change had not existed
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) cope with changes positively; and (ii) grasp opportunities resulting from changes for improvement.	
Remark		

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Monitor, control and update project schedule	
2. Code	ITSWPM504A	
3. Range	Monitor and control project schedule, and update the project schedule accordingly, in order to ensure timely completion of a project [Project Management – Project Time Management]	
4. Level	5	
5. Credit	2	
6. Competency		Performance Requirement
	6.1 Understand the critical path in schedule	Be able to know the possible critical path in a schedule and the corresponding control factors
	6.2 Conduct Schedule Control	Be able to ▪ define the procedure by which the project schedule may be changed ▪ implement a schedule change control system ▪ integrate schedule activities with the overall change control system ▪ determine the need for a schedule change ▪ determine the magnitude of the schedule change and the need for re-establishing the baseline ▪ determine overall plan adjustments resulting from schedule updates ▪ determine the need for schedule fast tracking or crashing ▪ initiate corrective actions to ensure that additional schedule changes are minimized ▪ integrate approved schedule changes with other project control processes
	6.3 Control progress in respect to the plan	Be able to define/Monitor/Review/Measure tolerance, product descriptions, work package authorization, quality control, project issues, project change control, risk log, checkpoints, and so on
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) monitor project progress; and (ii) exercise adaptive controls to minimize time variance.	
Remark	Co-requisites: ITSWPM605A, ITSWPM607A, ITSWPM508A, ITSWPM510A, ITSWPM520A	

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Manage the execution of a project quality management plan
2. Code	ITSWPM509A
3. Range	Execute the project quality management plan and manage issues related to project quality to ensure that a project will satisfy the needs for which it was undertaken [Project Management – Project Quality Management]
4. Level	5
5. Credit	2
6. Competency	<u>Performance Requirement</u> 6.1 Understand principles and techniques of project quality management and project quality assurance. — Be able to execute a project quality management plan 6.2 Conduct quality assurance — Be able to ▪ perform project quality control testing and measurement ▪ determine the benefits/costs of project quality efforts ▪ document project quality outcomes in a format suitable for comparison and analysis ▪ identify and implement actions needed to increase project effectiveness and efficiency ▪ document lessons learned for improved performance ▪ implement quality improvements using the project change control processes ▪ execute project quality control, assurance, and improvement processes 6.3 Report quality and related issues together with documentation as needed — Be able to ▪ report the quality review and incident report, and capture in a quality log such as Change Log and Risk Log ▪ provide sufficient and appropriate details in the respective document such as Exception Report, Follow-on Action Recommendations 6.4 Exhibit professionalism — Be able to formulate an appropriate approach in conducting quality assurance based on practical requirements of an organization's specific environment
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) conduct quality control and assurance in accordance with the project quality management plan; (ii) document project quality outcomes for comparison and analysis; and (iii) identify and implement quality improvements.
Remark	Pre-requisites: ITSWPM614A

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Conduct source selection and/or contract development
2. Code	ITSWPM523A
3. Range	Conduct source selection and further contract development in project outsourcing [Project Management – Project Procurement and Contract Management]
4. Level	5
5. Credit	5
6. Competency	Performance Requirement 6.1 Have knowledge of various evaluation methods — Be able to apply an appropriate evaluation system to the received proposals such as weighting system, screening system and independent estimates. 6.2 Identify contract concerns — Be able to rely upon methods to identify: ▪ project warranties ▪ liabilities ▪ indemnity ▪ insurance clause-related activities 6.3 Rank order to all proposals professionally — Be able to make ranking to each proposal according to the criteria as listed in the procurement management plan 6.4 Make contract negotiation with the bidder according the rank sequence — Be able to clarify any unclear points in the received proposal from the bidders and negotiate with them on the terms and conditions according to the local law 6.5 Reach mutually agreement with the bidder — Be able to make agreement on the structure and requirements of the contract prior to the signing of the contract (see remark)
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) make a fair selection for a successfully bidder; and (ii) get consensus and understandings on those important terms with the successful bidder for drafting the contract.
Remark	Subjects covered generally include, but are limit to, responsibilities and authorities, applicable terms and law, technical and business management approaches, contract financing and price.

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Monitor and control project execution	
2. Code	ITSWPM605A	
3. Range	Monitor and control project execution, and update the project plan accordingly so that all elements of the project are properly carried out [Project Management – Project Integration Management]	
4. Level	6	
5. Credit	1	
6. Competency		Performance Requirement
	6.1 Understand the requirements of integrated change control	Be able to ▪ understand change request procedures and documentation ▪ understand the functions of change control board or other governing bodies ▪ understand change management procedures ▪ have knowledge of change control system ▪ understand configuration management procedures
	6.2 Conduct integrated change control	Be able to ▪ verify that a change has occurred ▪ determine that a change is needed and the change request documentation has been properly completed in accordance with the defined procedure ▪ adhere to the steps by which official project documents may be changed ▪ determine whether variances from the plan require corrective actions, need new or revised cost estimates, result in a modification of activity sequences, or require the development of additional risk response alternatives ▪ utilize the powers and responsibilities of the change control board or other governing bodies ▪ document and implement procedures to process changes that may be accepted without prior change control board review or other governing body ▪ employ proactive, structured change management procedures to properly influence a variety of project stakeholders ▪ utilize the organisation's change control system ▪ complete project plan modifications, including integration with various project baselines ▪ utilize configuration management or equivalent procedures to integrate change across all areas of the project ▪ provide definition on the process, authority levels, integrity of change (see Remark 1)

	6.3 Direct a project with the focus on controlling project work	Be able to ▪ provide controls overview ▪ define controls for project start-up, progress and closure ▪ review and assess project progress and status, and report highlights ▪ capture, examine and escalate project issues ▪ take corrective actions
	6.4 Conduct integrated change control in a professional way	Be able to ▪ perform the activities of integrated change control in an efficient and effective manner ▪ obtain approval from stakeholders
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) monitor and control the execution of project plan in accordance with the project plan developed; and (ii) manage changes in accordance with the organisation's change request procedure.	
Remark	1. Integrity of change includes but not limited to: a) Benefit/business case driven b) Risk log c) Time/cost/risk function balance; and d) Whether the change is part of a business program. 2. Co-requisites: ITSWPM607A, ITSWPM504A, ITSWPM508A, ITSWPM510A, ITSWPM520A.	

Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Formulate IT strategies and policies	
2. Code	ITSWSM603A	
3. Range	Formulate IT strategies and policies for an organization to support its approved business strategies and policies and to cover areas including resource optimization, business alignment, and information security [Strategic Management – Strategy Formulation]	
4. Level	6	
5. Credit	4	
6. Competency		<u>Performance Requirement</u>
	6.1 Understand the business strategies and policies of an organization	Be able to know the business strategies and policies of an organization with respect to business-IT alignment and enablement
	6.2 Understand international standards and regulatory requirements	Be able to understand international standards and regulatory requirements
	6.3 Understand related issues in information security and related laws of intellectual property	Be able to know related issues in information security (e.g. data security, authentication, integrity and privacy) and related laws including copyrights and IP rights etc
	6.4 Formulate IT strategies and policies of an organization	Be able to formulate IT strategies and policies of an organization to support its approved business strategies and policies including resources optimization, business alignment, and information security in compliance with necessary international standards and regulatory requirements
7. Assessment Criteria	The integrated outcome requirements of this UoCs is the ability to formulate IT strategies and policies for an organization to support its approved business strategies and policies, with profound considerations of resources optimization, business alignment, information security and regulatory compliance.	
Remark	Pre-requisite: ITSWSM602A	